O2 business

Managing the risks in an ever-changing threat landscape

Why focusing on people makes a difference to your cyber security

Cyber attacks are evolving, and that's a concern for everyone.

What does a lack of security really mean today? There's no one singular answer. It's different for every organisation. From a loss of credibility and impact to brand, to increases in fines for breaches of regulations such as GDPR, or a complete shutdown of a corporate network.

One thing is certain – it's not when someone will attempt to attack you, but how well you can minimise the impact to your organisation. It's why cyber security is no longer just an IT concern, but is being recognised as a wider business issue, with responsibility needing to be shared by everyone. Many larger organisations now have a dedicated C-level security executive. Cyber security is no longer just a technical problem to solve, but a strategy that involves every aspect of the organisation, and everyone needs to play their role.

So with an increased business focus on cyber security, how can you be sure your organisation is getting the protection it needs?

The answer still needs to start with technology – making the right buying decisions and implementation choices can significantly reduce the risks you face. But at O_2, we see many organisations missing a key component in their security strategy – their people. As attack vectors become more targeted by relying on personal details and habits to succeed in their acts of deception, the way an individual in your organisation responds to a threat will determine the impact of the attack.

Get your people on your side

The way your people work together to support and respond is now more critical than ever before. Whether they work in sales, marketing, finance, as a field engineer or anywhere else across the business, everyone has a role to ensure cyber security is front of mind, not just the IT department.

Understanding the ways that people think and react is critical. People have their own job roles to complete, and not everyone has the time or ability be a cyber security specialist. But with the right processes in place, everyone can have a level of cyber confidence, knowing what they should do and when, helping to ensure the correct levels of response and action are taken.

The role of people in cyber security is something we've been focussed on for our own workforce across O_2. Here's our view, together with insights from the UK government's National Cyber Security Centre: part of GCHQ set up to protect critical services from cyber attacks.

The role of people in cyber security is something we've been focussed on for our own workforce across O_2. Here's our view, together with insights from the UK government's National Cyber Security Centre: part of GCHQ set up to protect critical services from cyber attacks.

The changing threat landscape

Always-on mobile devices, remote access to data, an increase in the number of connected devices to an organisation's networks, and social platforms to help keep connected to colleagues and industry peers, along with a host of other technologies, are giving organisations the chance to innovate and grow. It's opening up the world and creating great new business opportunities. But it's also an opportunity for the 'bad guys' to take advantage.

Cyber threats were once the product of a small, cottage industry, typically with more of a focus on the challenge of infiltrating an organisation's network, rather than the commercial opportunity it now represents.

The image of the lone teenager hunched over a PC in the middle of the night might be derived from 80's films like War Games, but today's cyber attacks are the products of a highly profitable, results-driven global industry, full of innovative hackers working hard to create ever-changing digital threats delivered via unexpected sources.

After a huge focus on ransomware in 2016/17, this 'marketplace' now appears to be in decline. There have been fewer infections and a significant reduction in ransom demands: the average in 2017 was down to $522, less than half that of the previous year, probably because operating system vulnerabilities are becoming more difficult to identify.[1]

And so hackers are finding new ways to exploit organisations. One emerging threat is supply chain attacks, where hackers infiltrate a software developer or supplier to gain access to source code or an update mechanism, adding in their malicious code. Software is built and released by trusted vendors, their apps and updates are signed or certified. So any malicious code then runs with the same trust and permissions as the application – and the end user is unaware that they've just opened their device to the hackers' hidden threat.

In 2017, there was a

200%

increase in malware implants into an organisation's software supply chain.[1]

1Symantec, Internet Security Threat Report 23, 2018, www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

The social media effect

The proliferation of social networks has helped make personal information far easier to access. So too has the increase in publicly available information, such as the reporting structures, systems or technologies being used in your organisation. These insights were far more difficult to access in the hard copy times of decades past. As a result, we are seeing an increase in spear phishing, where hackers use highly personal details and insights to convince people to give them access to their accounts, or send them (exfiltrate) data. It's now the top infection vector, used by 71% of organised groups.[1]

O_2's head of cyber security Tom Mullen agrees it's a huge concern. "The technology is there now to make a phishing attack highly believable. A simple example is access to a company's billing system. A quick search of LinkedIn will tell you who works in the billing department, and their biography and skills listings will often give you key insights into what billing platform they use. Combine this with publicly available information about email address formats and known platform vulnerabilities, and you've got all the information you need."

Cyber security today

The number of cyber threats targeting organisations continues to grow at a rapid rate and with ever increasing levels of sophistication.

8,500%
increase in detections of coinminers on endpoint computers

600%
increase in overall IoT attacks in 2017

1 in 13
web requests lead to malware, a **3%** year-on-year increase

But vulnerabilities are increasingly hard to exploit, so we're seizing a change in attack vectors.

200%
increase in attackers injecting malware implants into the software supply chain to infiltrate unsuspecting organizations

46%
increase in the number of ransomware variants but a **70%** decrease in ransomware families, suggesting a shift to focus on new, higher value targets

54%
increase in mobile malware variants

24,000
malicious mobile apps blocked by security software each day (on average)

And attacks are becoming more personal.

No.1
infection vector is spear phishing, employed by **71%** of organized groups

183%
increase in spear phishing makes it 2018's fastest growing threat

63%
of mobile grayware leaks the user's phone number

Source: Symantec, Internet Security Threat Report 23, 2018, www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

The top attack vectors and what they mean

#1
Spear phishing

An attack that targets an individual using personal knowledge in order to convince them to click on a malicious link, or to divulge (exfiltrate) important information.

#2
Watering hole attack

Compromising a website that is likely to be visited by the attack targets. For example, if someone works in the financial services sector, the hackers may infect a financial news forum.

#3
Supply chain attack

Infiltrating the systems of a trusted software developer or supplier to make malware widely available through its updates, which usually run as trusted apps or updates.

#4
Web server exploits

Using known vulnerabilities in SQL-based web applications to send malicious commands that exfiltrate important or sensitive data from the SQL database.

Source: Symantec, Internet Security Threat Report 23, 2018, www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

How user-friendly is your IT security?

With cyber attacks becoming more personal, how much of the responsibility lies with your employer, and how much should lie with us as individuals?

For a long time, the role of IT security has been to put in place technological solutions to secure an organisation such as firewalls, software and firmware upgrades to address security vulnerabilities and other appliances to inspect network traffic or manage data loss prevention. A new threat appears and, if the business can afford a solution, it makes the purchase. The IT team works out how to implement or install it, then gets people to use it.

But National Cyber Security Centre analyst Ceri J says this can be counterintuitive. "The organisation believes it's becoming safer but, actually, it's just building in complexity. And when security information and systems are fragmented, people don't always know where to go.

Procedures aren't consistent, or don't quite align, and people don't know what to do. So they do their own thing. Most of the time it works out fine. But sometimes it doesn't."

Tom Mullen has observed first hand how layering technology isn't always the best solution – and why organisations should be looking at security by design. "Many organisations invested in VPNs as mobile working took off, and many of them are still using it. But if it's easier for people to upload and store information in their personal cloud accounts than to connect to the VPN, even if it's not as safe, then that's what they'll do. Because most people just want to get on and do their jobs. It's why we now provide securely authenticated network connections across our CAS(T) accredited networks. It means staff can connect seamlessly and securely to work servers without the overheads and complexity of VPNs," he says.

It's important to understand that everyone within their organisation has their own core role, be it in finance, marketing, front of house or back of house support and so on. We can't expect everyone to be a cyber security specialist.

Security by design

At O_2, we understand the value of security to our customers, and the importance of making it as easy to use and manage as possible. Not only because we need to ensure we keep our own staff and customer information safe, but that the team that runs our own cyber security operation is involved in helping deliver the solutions we deliver to our customers. We're still the only provider to have received the government's stringent CAS(T) security certification for both our fixed and mobile networks, giving organisations the reassurance that their data is kept safe wherever it travels.

Security by design has helped Surrey Police and Sussex Police forces to save nearly two hours of admin per shift, per officer. We've provided frontline officers with secure, real-time access to a number of their databases, from both forces, on mobile devices. Using preloaded apps, officers can continue their tasks seamlessly from any location. It's also generated an estimated £7m in annual savings for each police force.[2]

2 Surrey & Sussex Police – Digital Policing, www.o2.co.uk/enterprise/insights/surrey-police-and-sussex-police

How can you improve your security?

Build your foundations

"You can stop a huge number of threats if you get the basics sorted. Web filtering, patching, blocking as many threats as possible. Lifecycle management too – if you know a solution is going end of life in three years' time, make sure you have a replacement plan. Then you can start to be more proactive and start planning for the specific risks your business faces."

Tom Mullen
Head of cyber security, O_2

The biggest challenge for most large organisations is that they still see risk on a component level.

Ceri J says "Companies tend to focus on the latest risk, or how to improve a particular piece of security technology. They don't often look at a business holistically, and they don't really know how everything interacts. Understanding the complexity of a big business is hard. Even people with experience of doing risk assessments rarely do it on that scale."

But for an organisation to remain safe in today's threat landscape, it must deliver a step change in security.

Many organisations know they need to become more people-focused. But Ceri says that it's often for the wrong reasons. "They see that people aren't adhering to processes and that leads them to see these colleagues as an inside threat. However, the organisation isn't judging how usable its security solutions are. And if a security solution is useful, but not usable, then no one will use it."

The value of just culture

There's a real learning opportunity from the area of 'just' culture, a term that comes from the way many organisations in the safety sector operate. The foundations of a 'safe and just culture' are fairness, openness and learning – and that includes honest, two-way feedback. People aren't blamed for mistakes, instead there's a focus on what led to the incident, and how it can be fixed to prevent the same thing happening again.

Ceri explains how the traits of just culture can benefit IT security. "It helps organisations to build a culture where security is part of everyday life, breaking down barriers between 'them' and 'us', and encouraging questions and discussion. Policies can be overwhelming, whereas just culture encourages information that's easy to find and understand.

"We suffer from security experts thinking everything is easy. But when we engage with people, 'easy' depends on the person, situation and context," Ceri says.

How do you tell your security story?

The safety sector also offers up lessons in good communications, according to Ceri J.

As Ceri explains, "Organisations operating in the safety sector don't recognise IT security as a distinct activity, because sending out a different set of messages would detract from their core safety messaging, which increases risk. Instead, they integrate security into the safety messaging that already exists."

It's not just the number of communications you're sending out, what you're saying and how you deliver the message is key to how it's understood.

Does your story resonate?

Ceri says, "You need to make things relatable to the person, and not scary – which is a real risk with a security message. You need to ask yourself: How important is my message to this particular person, in this particular job role? Am I telling them a culturally relevant story? Am I telling them something they can relate to, and therefore understand?"

Ceri isn't surprised that most organisations don't tell good security stories. "It's accepted in marketing that you'll get a better response if you target people with the right message, using the most appropriate tools and techniques for their segment. It's no different for security messaging, but the majority of people involved in IT departments won't have had access to the same level of 'marketing' awareness or training."

Cyber comms at O_2

"O_2 has circa 6700 employees working at sites around the UK, including our Slough headquarters and branch offices, a large number of remote workers, and a retail shop network of over 450 stores.

"We use Workplace by Facebook as our communication tool, sending out notifications and details about cyber security. We find it's the most effective method, because we're integrating security messaging into a tool our people are already using for work every day.

The format is relatable, and the messages can take on more of a familiar and engaging tone to help provide the information our people need to know. For more urgent issues, we also send voicemails to people's phones, and put banners on the intranet.

"It's important to deliver our messages in a highly engaging way. For example, at the start of May we use a Star Wars theme (yes, 'May the Fourth be with you'…) as a way to get across an important message. And we also learn from the results. If a particular communication doesn't work, we'll adapt it next time."

Tom Mullen
Head of cyber security, O_2

Are you short of security expertise?

In a recent survey by McAfee, it was estimated that there could be as many as two million cyber security positions unfilled by the end of 2019.[3]

Your cyber security is important and you need the right people. But it can be hard to recruit people with the right qualifications and experience in today's fast-changing threat landscape.

Tom Mullen suggests it could be time to revise your recruitment procedures. "Cyber security is fundamentally a business-wide issue. It needs to involve everyone in an organisation, and be embedded in all your roles. Too many people still think it's a technical role – and that can lead to bad recruitment decisions." he says.

At O_2, we believe there are a number of ways you can address these challenges.

Recruit from within

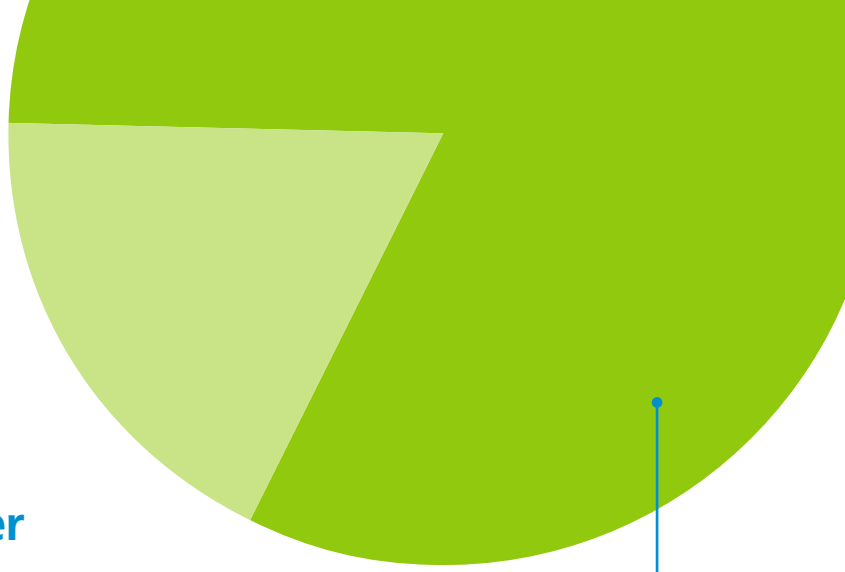
It's what we do at O_2. Our people already know our business, and it is often easier to give an existing colleague technical training, if they need it, than to teach a new recruit everything they need to know about the organisation and its culture.

Focus on retention

Keeping trained and valued people saves time and money. But it's not just about salary – at O_2, we find that our security people rate flexible working, training programmes and career progression more highly than money.

Diversify

And outsource where practical. Organisations like O_2 as part of Telefónica Group are at the forefront of cyber security research and development, with a global security network and R&D programme. With a range of security solutions, we provide the cyber security support an organisation needs to complement their existing IT teams.



82% of companies reported a shortage of cyber security skills and, of these, **71%** believed that the shortage was doing their business direct and measurable damage.[3]

3 McAfee, Hacking the skills shortage, 2017, www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf

Ready to focus on people? Start here.

The benefits of a people-focused approach to security are clear. But for many organisations it's a significant change in thinking. Meanwhile, some businesses think they're already running a people-focused campaign – but they're actually adding to the problem.

"Many organisations leverage all their security information into an awareness training session or package. But it delivers too much information at once, can be complex to understand – and it's rarely updated, even as the threats change," say Ceri J.

So if you want to make the move to people-focused security, how can you start? Here's our suggested steps:

#1. Be clear on your goals.

Look at what your organisation wants to achieve against your key security issues, and resolve any conflicts between them.

#2. Prioritise what's most important.

If keeping a PIN secret is critical in your organisation, focus on it. Don't confuse people with messages about insider threats, or they'll forget your key message.

#3. Make messages relatable.

You'll get better results if people can see the impacts of their actions. Show people how clicking a compromised link in email could result in them losing their data through ransomware, or giving their banking password could lead to an empty bank account. And send messages in whatever format is most appropriate for them.

#4. Start small and learn as you go.

Treat security as an iterative process, not a big bang. Work your way through steps 1 to 3 and see what happens. Learn what worked well, and what didn't. Then adapt your strategy and continually engage as part of an ongoing programme.

Want another view on your cyber security strategy?

Could a focus on people help you to deliver better security?

Tom Mullen, head of cyber security, Telefónica UK

Tom Mullen is Head of Cyber Response and IT Security for O_2/Telefónica UK.

He is responsible for securing the company infrastructure as well as incident handling and cyber investigations. Tom has served on the Forum of Incident Response and Security Teams (FIRST) board and steering committee for four years and has presented to the UK Government select committee on Cybercrime in the House of Commons, G8 Cybercrime Workshop on Terrorism, CNI Plenary Panel on Cyber Security, Microsoft Bot-Net Task Force, Europol and has provided advice and guidance on numerous EU and industry initiatives.

Ceri J, security analyst, National Cyber Security Centre

While working in IT support in the NHS, Ceri started to become interested in how people use computers and IT in the work environment. It eventually led to her working for the NCSC with a focus on people-centred security. She carries out research internally and takes part in field research with academic partners, developing views on the perceptions of security and finding new ways to support people using technology.

Published in March 2019. All information is correct at time of going to print. Telefónica UK Limited. Registered in England no. 1743099. Registered Office: 260 Bath Road, Slough, SL1 4DX

O_2 business