CYBER SECURITY

BUILDING, IMPLEMENTING AND MAINTAINING AN ONGOING SECURITY PROGRAMME TO REDUCE CYBER RISK

SHAPING YOUR CYBER SECURITY STRATEGY

A GUIDE FOR FORWARD-THINKING ENTERPRISES

STRATEGY GUIDE

Softcat

INVESTING IN THE FUTURE

Having a long-term strategic view of cyber security, rather than a point-in-time perspective

By Matthew Helling, Head of Cyber Security Services, Softcat

Almost everyone is aware of cyber security today. It's high on the agenda of many enterprises – well up there with green objectives. And just as enterprises have to be seen to be striving towards a carbon neutral future, they now have to be able to demonstrate their focus on cyber security too.

Indeed, cyber security is mainstream media news and big brands increasingly want to make us aware that they have dedicated security teams. There's a good reason for this; credibility.

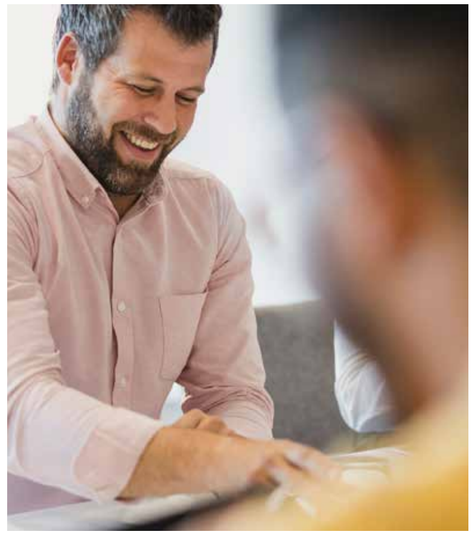
Most people today – businesses, customers and consumers – have an acceptance of risk. We generally accept that, at some point, an organisation can be compromised. This can be small and innocuous, or it can be damaging to all involved. Nevertheless, how an enterprise handles such an incident speaks volumes about their credibility.

What I have seen is that organisations have been able to recover from compromises if they have the right processes in place. If they can rapidly identify what data was taken, when it was taken, how it was taken and explain how they'll stop it from happening again in the future, then they stand a great chance of limiting reputational damage. However, at the other end of the scale I've seen organisations that don't have the same response to the same situation – and they're quickly depicted as negligent.

SHOWING THAT YOU'RE A SAFE PAIR OF HANDS

At Softcat, a lot of the conversations we're currently having are around preparing organisations to react, respond and adapt to compromises in the most responsible and effective way possible. We can help organisations prove themselves to be a safe pair of hands – and use this positive reputation to their advantage. Because today, it's a valid strategy to use an investment into a cyber programme to successfully self-promote.

In a competitive scenario, those who can demonstrate that they are taking cyber security seriously can put themselves ahead of those who can't. Investors, customers and consumers will buy into the perceived assurances. And with security as one of the key decision-making factors today, it's wise to show off your credentials.



INVESTING IN CYBER SECURITY

At the IT level, managers and directors are working hard to keep the lights on and enable workers to carry on working. Their perspective is understandably point-in-time; it has to be. However, at the board level, there's a need to identify a long-term view of remediating and removing risk to move the business forward.

It's also important to know what happens next. When a new solution is in place, how do you resource and manage it against the available budget? What's the next thing to consider once it's up and running? And in what order do you do it?

It's critical for you to understand, from a risk perspective, what the profile of your organisation looks like – and how you can reduce it over a period of time. Moreover, you need to know the cost associated with it and the tangible benefits available.

The challenge here is that with traditional investments in new people and platforms, it can be very difficult to see the on-going value. However, by using a service partner that allows you to consume services based on actual usage – providing SLAs with tangible assurances – then it's far easier to feel confident in your investment.

Therefore, with this in mind, I believe there will be a shift in the consumption of cyber security services. And I think the wider market needs to move closer towards paying for usage as opposed to estimating the cost of worst-case scenarios – providing the flexibility and scalability we all need.

INTRODUCING OUR APPROACH

Many enterprises are currently defensive in their approach. They're investing in cyber security at a particular moment because they've identified a potential area of risk. But at Softcat, we're here to help enterprises act more offensively; we can help you to pragmatically understand how to address risk, and we create programmes that let your customers know you're actively investing in this area.

This guide has been created to explore some of the key considerations around cyber security in the enterprise sector today – and provide you with practical advice to take proactive steps forward.

WHERE TO TARGET YOUR EFFORTS

WHAT EVERY ORGANISATION TODAY SHOULD AIM FOR

Graham Charlton
CFO, Softcat

To echo the sentiments shared by Matt, I'd like to briefly elaborate on where I believe cyber security investment can be most effective within an organisation today.

At Softcat, we made the decision to take ownership of our own cyber security delivery well over three years ago. With the aim of developing and working towards a long-term plan, we built a dedicated team to take responsibility for our efforts. Since then, as Softcat CFO, my priorities have been to establish and maintain an internal audit programme that monitors progress regularly; and implement the end point security governance of all our devices.

What drove us to create this team? Fear of compromise, perhaps. Regulatory requirements, yes. Awareness of increased threat, certainly. And a realisation that reputational damage caused by security breaches can be devastating. Thankfully, it's fair to say that our efforts have so far been successful. In fact, in my opinion, any organisation looking to improve their cyber security should have a good internal team that they can trust.

Even when budget doesn't allow for a full internal team, having someone responsible for managing third party security providers is essential. This internal presence offers a vital link with the C-suite, who may not understand the detail required to make the most informed security decisions – and it helps to build the business case for further, targeted investment.

In order to provide multiple levels of assurance, it's important to then choose the right security partner – someone who can provide assessment, procurement and management services to support the internal team. By its very nature, cyber security is hard to measure in terms of the value it brings to a business. Equally, the ever-evolving landscape makes things even more challenging. Therefore, harnessing the expertise and experience of a trusted partner is crucial.

Today, it's easy to over-invest in cyber security. An organisation can invest thousands into security products that promise to overcome all their challenges. However, if you don't know how to implement those products properly, it's easy to waste money. Therefore, I believe it's important to use the expertise of your internal team and trusted partner to invest in the right solutions; invest in training your people, who inevitably pose the greatest risk factor; and then invest in managing your processes to ensure that they're being followed correctly.

While it's impossible to mitigate 100% of the risks, intelligently managing cyber security in the most cost effectively way is what every organisation today should be aiming for.

Contributor overview

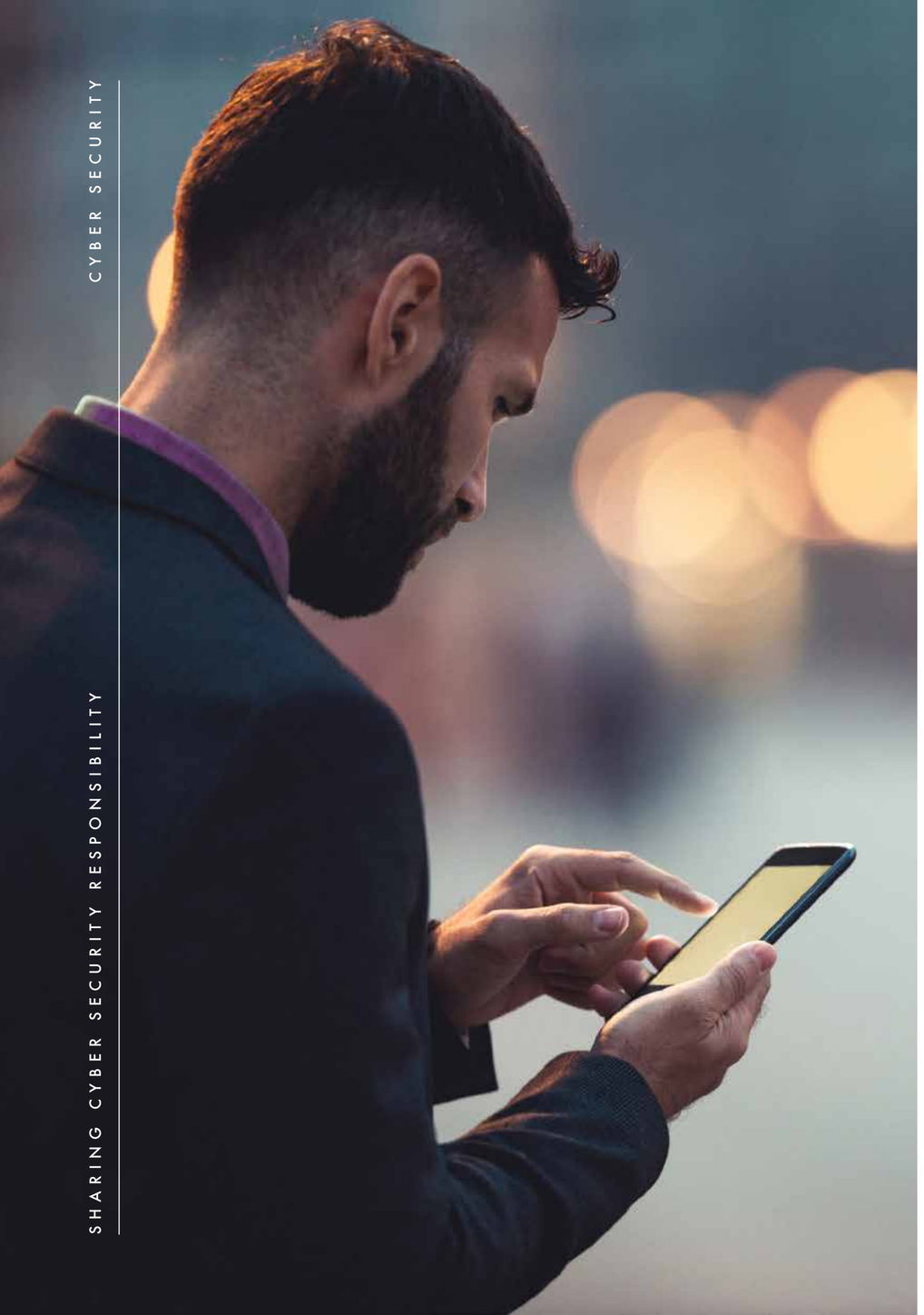
To help inform this strategy guide, we've held in-depth conversations with two of our experts to talk about the key areas that enterprise sector organisations need to consider when building a cyber security strategy. Both offer a wealth of experience within the security space. And over the coming pages, we've shared their insight, opinion and expertise in order to help you overcome your cyber security challenges.

ADAM LOUCA
Chief Technologist – Security, Softcat

Adam focuses on developing, engaging and transforming Softcat's strategic customers' cyber security approach. In addition, he also runs Softcat's cyber assessment services business, which helps customers understand and improve their cyber security.

SEAN HUGGETT
GRC Consultant, Softcat

Sean specialises in governance, risk and compliance, including data protection, security risk management and ISO 27001. He has helped Softcat customers prepare for GDPR, NIS, ISO 27001 certification and other industry security standards.



SHARING CYBER SECURITY RESPONSIBILITY

Digital initiatives aren't just for the IT department, they're for everyone in the business

By Adam Louca, Chief Technologist – Security, Softcat

To be relevant to customers today, organisations need to demonstrate good cyber security practices because anything below standard is quickly becoming societally unacceptable. This is driving positive change within enterprises everywhere, as they look to uphold their reputation.

As a consequence of this evolved perception, the commerciality of cyber security as a business conversation is drowning out traditional talk of risk avoidance. More and more organisations are ceasing to think solely about the regulatory obligations they need to meet, and are beginning to realise that cyber security can be a differentiator for the supply chain – attracting customers and fresh talent alike.

No longer is cyber security a tedious box-ticking exercise for the tech team to deal with; it's front and centre of the business. And demonstrating your cyber security credentials is becoming as important as your brand's culture or operational excellence – so, you need to be proactive rather than reactive in your approach.

DEFENCE VS OFFENCE

Understanding how to use cyber security to make your business better is crucial. Are you purely looking to avoid risk – defensively using cyber security to react to issues? Or are you one of the many organisations beginning to realise the benefits of being more offensive in your approach?

I've seen a lot of organisations continuing to operate defensively when it comes to their security. They have a mindset of having to do it, rather than wanting to do it. And everything is seen through the lens of cost, rather than value. However, with an offensive approach, organisations are able to demonstrate their operational excellence – enabling them to stand apart from their competitors.

Proactively tackling cyber security head-on and promoting your cyber security capabilities externally can help you acquire customers – or displace other businesses who have dealt badly with cyber security incidents. Cyber security can also provide a solid foundation for you to consume new technology; you can invest to differentiate, and you can adapt to new innovations that come along. Getting ahead with cyber security can help to prepare your business for tomorrow, rather than just fixing problems today.

CYBER INVESTMENT: THE START OF VALUE REALISATION

The main thing to understand is that cyber investment is only the start of value realisation. Making an investment doesn't instantly trigger value – you must implement and embed the technology before the value realisation begins. However, in my experience, many C-level executives from a non-technical background see a singular cyber security investment as the bit that fixes the problem; it's not.

Value is distributed across all of your security solutions, as opposed to through individual investments, which means the integration of your technology is key. This integration is also important because gaps in technology must inevitably be filled with people, which is why organisations find themselves with spiralling staff costs – and a lack of value realisation.

Indeed, one of the big challenges organisations face is the recruitment and retention of skilled staff; people represent the main investment for professional services firms. But the good news is that you can leverage technology to bridge the gaps, do more work, and bill more hours. This is why, at Softcat, we work with many legal firms who are building their own apps. It means that rather than hiring lawyers, they can instantly dispense legal advice and generate more interesting work.

CREATE YOUR OWN ECOSYSTEM

From a business perspective, the days of keeping everything in-house are fading fast because building an ecosystem of trusted partners can benefit your own organisation immensely. Following the impact of COVID-19, many organisations have had to partner with specialists to enable business continuity. From agile retail fulfilment businesses, to last-mile logistics firms, and SEO agencies, these ecosystems are proving valuable for organisations of all shapes and sizes.

The digital-first business model has taken priority. And digitally integrated relationships with the people in your supply chain are no longer future fantasy; they're here and now.

THE NARRATIVE NEEDS TO CHANGE

It's fair to say that, traditionally, security has been communicated to boards in a negative way and there's little wonder some boards have been reluctant to invest. Scare tactics and fear makes it feel like you're spending on a problem that never gets fixed. Therefore, the narrative needs to change; we need to be more positive. What are you doing right? How are things getting better? What are the overarching business objectives and how does cyber security enable them?

Investment into cyber security should feel like spending money on the foundations of the business, rather than pouring it into a bottomless pit. A long-term strategy needs to be identified and cyber security needs to represent continual small improvements; rather than a quick-fix overnight change.

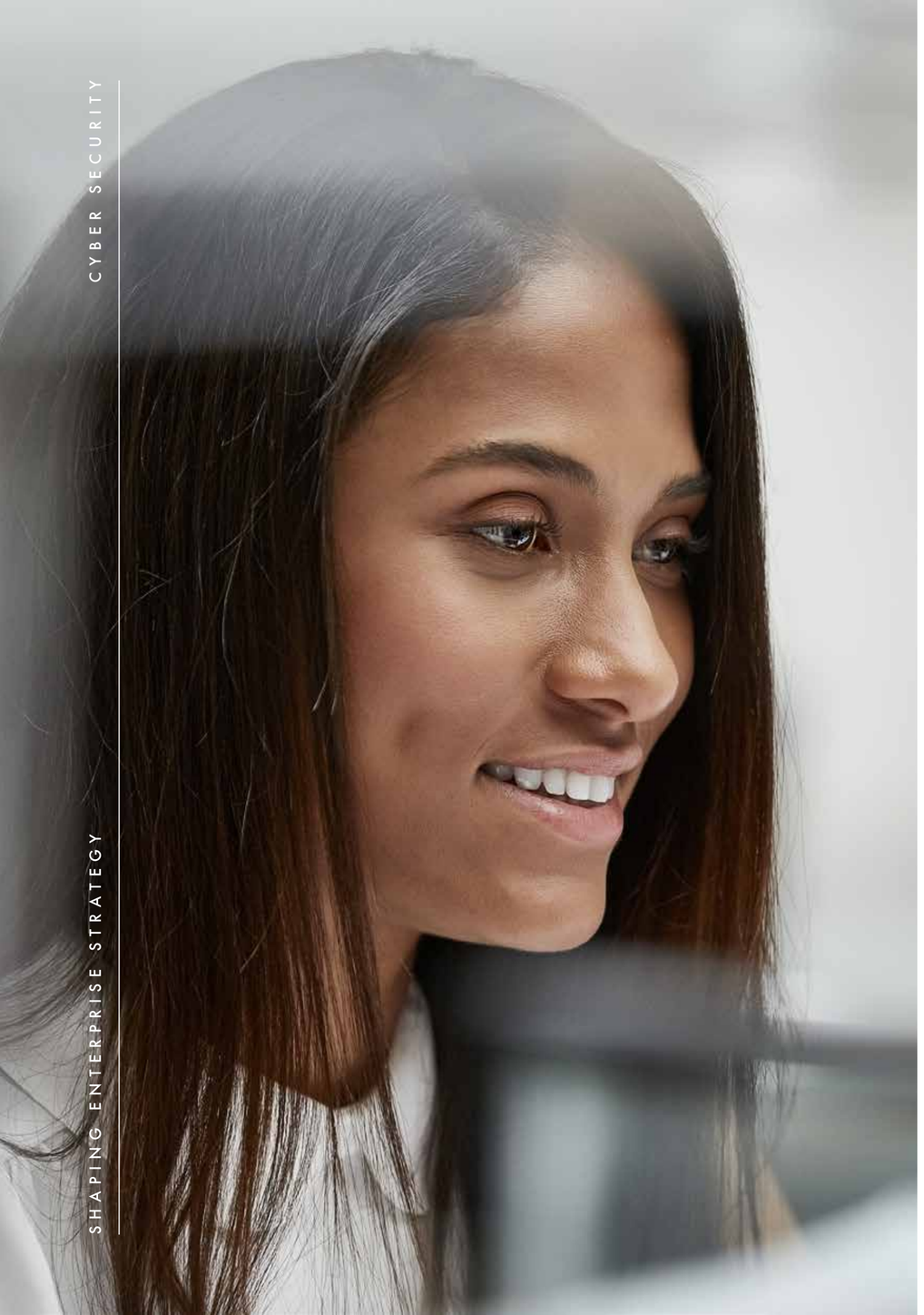
A lot boils down to mindset. It's not about the technology, or about the challenge; it's about making progress. You don't have to get your cyber security strategy perfect first time, you can instead improve iteratively along the way. It's a cliché, yes, but it's certainly a journey as opposed to a destination.

GETTING EVERYONE INVOLVED

Finally, it's important to reiterate that digital initiatives shouldn't be the reserve of the IT department. Every business is now a digital business – so everyone should be involved.

This is the reason we're currently seeing the rise of the Chief Information Security Officer (CISO). Forward-thinking boards recognise they need a peer who is invested in the overarching business strategy, but who are also able to provide a steer into the cyber and information security side of the business. They're there to make things happen, say 'yes' more often, and move things away from defence mode.

At Softcat, we support CISOs – and everyone else across the C-suite – to confidently approach digital transformation. We work closely with our customers to outline their objectives and work towards them, step by step. We take a pragmatic, risk-based approach. And we happily share the cyber security responsibility.



SHAPING ENTERPRISE STRATEGY

Why IT providers are becoming the business consultants to listen to

By Sean Huggett, GRC Consultant, Softcat

Everyone is digitally transforming. It's perhaps the silver lining to the COVID-19 cloud. But while more and more traditional bricks-and-mortar organisations are trying to put technology at the heart of their business, they don't always understand the security implications of doing so – therefore it's up to IT providers to guide them.

When embracing new technology, it's crucial to define what should security look like, including the technology, the management and the policies required to support change. This is why we're currently seeing a shift in the market dynamic of IT providers, who are becoming more like business management consultants in their nature – Softcat included. So, let's explore this concept further.

SPEAKING THE RIGHT LANGUAGE

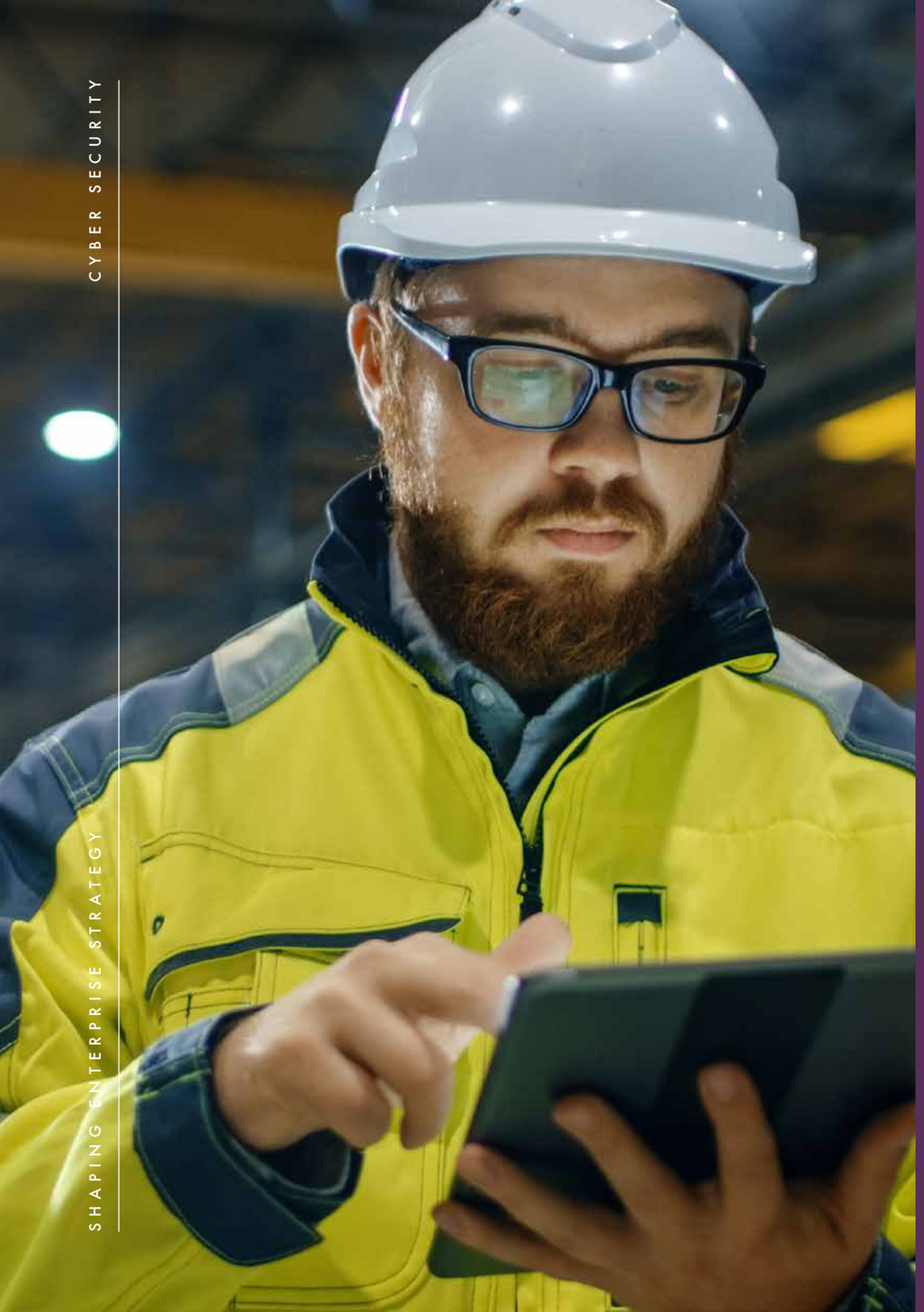
Today's C-suite understands that technology is more important than ever, but it can be hard for them to communicate successfully with their internal IT teams.

That's because the board needs to hear the business case for technology investment in the appropriate business language; they need to know the risk, the cost, and sometimes hear the truth from an impartial external voice.

Additionally, it's key to ensure an organisation's key decision makers understand the fundamental differences between information security and cyber security. Because while 'cyber' has become a catchy buzzword, the majority of risk is more likely coming from a lack of information security.

Information security can be defined as anything that puts confidentiality, integrity or availability at risk. This includes things like physical security (walking out of an office with paper documents under your arm), emails to the wrong people, loss of hardware and insider threats. In fact, there's more risk of employees doing silly things and making mistakes than anything else.

Cyber security, however, is what the media loves to talk about. It's a subset of information security; it's people looking to exploit weaknesses and take advantage of an organisation via internet connectivity. Either way, being able to communicate the business impact – and opportunities – of either cyber or information security is crucial.



GETTING A HOUSE ALARM AFTER YOU'VE BEEN BURGLED

Many organisations are increasingly looking at their information security management. Who's responsible? Who's accountable? And what is the target operating model around security? They're starting to recognise that they might not have an established lifecycle around security and that security measures are only being carried out when something goes wrong. In my opinion, this is a bit like getting a house alarm fitted only after you've been burgled!

Thankfully, however, the same organisations are learning that security is not a one-off thing, it's a continuous process. They're looking to establish the right policies and behaviours, and they're wanting to set the rules that meet the needs of the business.

This realisation and improvement is, in part, being driven by the wider supply chain. A lot of B2B organisations are in a stack with larger organisations that are heavily regulated and need to meet all kinds of requirements. This high level of security then percolates down the supply chain and everyone else has to up their game. Equally, many suppliers actively want to show they're on the same level of security as the major player to gain leverage and be chosen in competitive scenarios.

PROACTIVELY RECOGNISING RISK

With the mounting recognition of cyber and information risk at a non-executive level, large, publicly quoted organisations are increasingly adopting cyber security improvement programmes. This is, of course, a good thing. Consumer trust is key when it comes to cyber security and the media will trumpet any attacks, which in turn impacts reputation and share price. Consequently, there's a growing acceptance that it's beneficial to lead with a strong cyber story about how the business protects its data.

There's also increasing acceptance from organisations that potential attacks or compromises are now a matter of 'when' rather than 'if'. And they're starting to understand what steps they might need to take to mitigate the risks, minimise damage and take control of the PR post incident response.

All of these positives are what we should be focusing on. That's why, at Softcat, rather than picking out what's lacking within an organisation's security infrastructure, we help to optimise what's already there. And because it's almost impossible to secure everything at the same time, we also help organisations prioritise and put controls in place to overcome their challenges progressively. We support organisations to protect their information, secure the service that they offer to their customers – and ultimately help to shape their enterprise strategy.

Understanding how to address risk and take a positive approach

C-level decision makers within the enterprise sector must now learn how to share cyber security responsibility, leverage IT to shape enterprise strategy, and invest wisely in the long-term future of their business – it's perhaps the only way to remain competitive moving forwards. With this realisation in mind, here are the key pieces of advice to take away from the conversations we've had with our enterprise sector experts:

- **Have a long-term strategic view of cyber security** rather than a point-in-time perspective. It's critical for you to understand, from a risk perspective, what the profile of your organisation looks like – and how you can reduce it over a period of time.

- **Take an offensive approach** as opposed to purely defensive. Understand how to use cyber security to make your business better. Show that you're a safe pair of hands and demonstrate your operational excellence to stand apart from your competitors.

- **Put the right processes in place** to recover from compromises – learn how to rapidly identify what data was taken, when it was taken, how it was taken and explain how you'll stop it from happening again in the future to limit reputational damage.

- **Use cyber security as a solid foundation** to consume new technology. Invest to differentiate and adapt to new innovations that come along. Prepare your business for tomorrow, rather than just fixing problems today.

- **Understand that cyber investment is just the beginning** of value realisation and accept that an investment doesn't instantly trigger value – you must implement and embed the technology before the value realisation begins.

- **Integrate your cyber security solutions** to realise value across your estate. Be aware of the potential for spiralling staff costs and leverage technology to bridge gaps, do more work, and bill more hours.

- **Create your own ecosystem** of trusted partners and employ a digital-first business model. Form digitally integrated relationships with the people in your supply chain to enable short-term business continuity and realise long-term business benefits.

- **Change your mindset and approach cyber security more positively.** What are you doing right? How are things getting better? What are your overarching business objectives and how does cyber security enable them?

- **Speak the right language** and ensure that IT communicates the risk and costs associated with any changes. Understand the differences between information security and cyber security – and learn the impacts and opportunities of each.

If you're interested in the many ways in which Softcat can support your enterprise sector organisation, don't hesitate to get in touch. We'd love to learn about your current setup, and advise how best to improve upon it.

Email: **CyberServices@Softcat.com**
Or speak to your Account Manager today.

Softcat