CYBERFORT

Nothing gets past you with Cyberfort

The areas most businesses miss when it comes to cybersecurity

Keep them from becoming an attackers' greatest hit

If you were a cyberattacker, where would you strike? It may not be a pleasant headspace to inhabit, but it's an essential question to ask if you want to effectively protect your business. For many of your peers, the answer is technology. It's connected, very often mobile and absolutely essential. If you were a cyberattacker, that's where you would attack. So, that's where you should be spending your cybersecurity budget.

And with your technology secured, you're free to focus on operations and growth. Right? Most businesses would agree – and stop there. The reality is that cybersecurity can't be limited to just your technology. Just as your business is a complex web of people, processes and technology, so your cybersecurity approach must be, too. And even while you focus on operations and growth in all areas of your business, it's essential to consider how cybersecurity comes into play.

In this guide, join us as we explore some of the unexpected areas in need of cybersecurity – and show you how, by considering people, processes and technology together, you can make the most of your cybersecurity budget.

Nothing gets past you is a thought leadership campaign from Cyberfort – helping cybersecurity decision-makers fill knowledge and security gaps across their businesses. Stay sharp and find answers to even more of your colleagues' questions by visiting: **cyberfortgroup.com**

Look for opportunities where you are

So, where should you be spending your cybersecurity budget if not on your technology? You're probably already familiar with the areas – they're the places holding your attention right now.

Cybersecurity, like so much else, has become a business-wide responsibility. (That's why you're reading this guide even though you may not be a CISO.) That means it's up to everyone to ask themselves how cybersecurity could fit into what they're working on right now. Let's take a look at some trends in small and medium businesses and ask: What does this have to do with cybersecurity?

CYBERFORT

Our organisational structure is a bit up in the air right now

It's not unusual to reshuffle during periods of unexpected growth. But as key team members take on new roles and start building teams of their own, these changes can take some work.

What does this have to do with cybersecurity? Everyone needs to be held accountable for cybersecurity. But undefined or unclear organisational structures can make that accountability hard to track – and gaps in your hierarchy can leave holes in your digital defence. As you work on your organisational structure, consider creating a cybersecurity roadmap at the same time, so everyone knows their role and responsibilities.

CYBERFORT

We want to give existing and incoming employees options for flexible working

The rise of remote working has given employees more control over their work-life balance – even if it reduces the control IT teams have over protecting them.

What does this have to do with cybersecurity? Business leaders cite a number of reasons for preferring employees work in the office, but perhaps the most legitimate is cybersecurity. For them, the solution is to limit activities associated with risk – when they should be finding ways to reduce the risk itself. One solution is to introduce employee training in exchange for the freedom to work from home – making everyone aware of their own behaviours and outcomes.

CYBERFORT

We need to find ways of cutting costs – or at least stop them rising

Less a trend and more a state of being, the small and medium business's quest to cut costs – or at least hold them steady – will already have you looking in unexpected places.

What does this have to do with cybersecurity? You don't want to cut your cybersecurity budget. But could you be spending it more wisely? If you've got cybersecurity insurance, the answer is probably yes. This insurance isn't the be all end all – in fact, it's becoming normal for providers to withhold pay-outs from businesses that don't meet their demanding cybersecurity requirements. An effective way to cut costs without slashing security? Invest in your own cybersecurity measures instead of paying for coverage that, in the event of a breach, you may not be able to claim.

CYBERFORT

We need to innovate to beat the competition to new services and solutions

Wherever technology plays a role, so do your people and processes. After all, it's their expertise that makes innovation possible – and their experience that determines whether new solutions last.

What does this have to do with cybersecurity? Cybersecurity is often considered a barrier to innovation, but it doesn't have to be. By integrating security into the development process, you can reduce the risk of data breaches and protect valuable assets – a compelling competitive advantage in itself that also frees you to explore new opportunities with confidence.

CYBERFORT

We're trying to establish compliance but don't know which standards to aim for

Your industry may demand it – or your clients and customers may expect it. In any case, the combination of compliance and certifications your business requires is unique to you.

What does this have to do with cybersecurity? Regardless of the expectations of industries, clients or customers, there are some regulations every business should be meeting to protect its technology, people and processes. If you're looking to establish or boost your compliance, the following standards are great places to start:

- **ISO 27001** – Information Security Management
- **ISO 27701** – Privacy Information Management
- **ISO 22301** – Business Continuity Management
- **NIST** – National Institute of Standards and Technology
- **SANS** – Sysadmin, Audit, Network and Security

See how we've helped turn good cybersecurity into improved budget ROI

A leading digital print and document solutions provider came to us to help put its cybersecurity budget to better use. We uncovered some places that needed protecting that the client didn't expect – and imbued it with the confidence to grow in the marketplace. Here's how.

The challenge

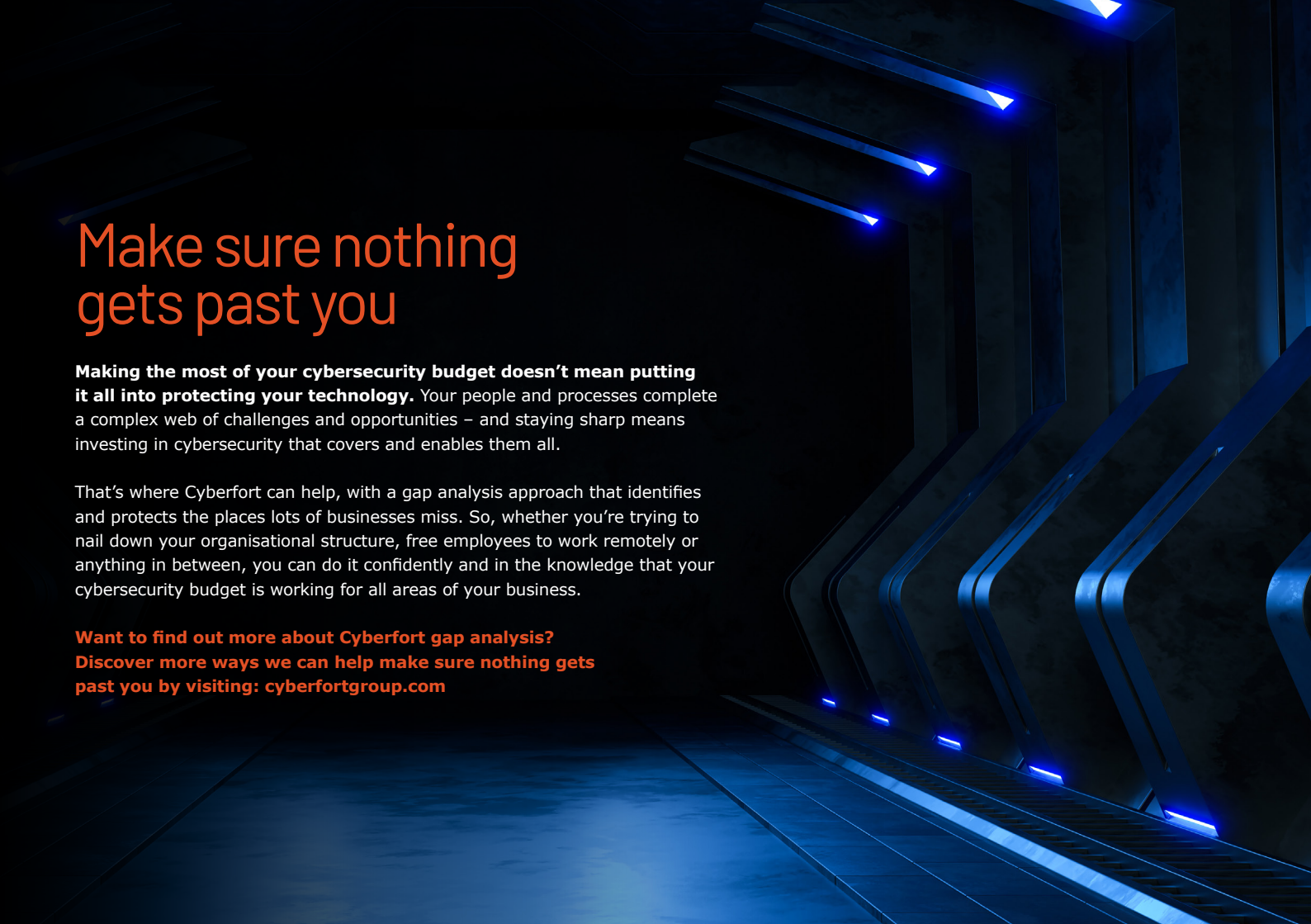
The client wanted to make bold steps forward to stay relevant in an increasingly competitive marketplace. But accountability for cybersecurity was undefined – with compliance a key customer sticking point.

The solution

We helped the client adopt the internationally recognised Information Security Management System standard ISO 27001 to demonstrate its commitment to cybersecurity to clients. The client was able to easily align to a customer's regulatory standard by mapping their ISO 27001 to the requirements.

The result

By focusing cybersecurity budget on areas aligned with its business goals, the client has achieved a major customer acquisition quickly, confidently and cost-effectively. And Cyberfort has taken on the role of governance and risk consultant for the client, ensuring ongoing visibility and reporting that maintains a level of compliance and keeps budgets from ballooning.



Make sure nothing gets past you

Making the most of your cybersecurity budget doesn't mean putting it all into protecting your technology. Your people and processes complete a complex web of challenges and opportunities – and staying sharp means investing in cybersecurity that covers and enables them all.

That's where Cyberfort can help, with a gap analysis approach that identifies and protects the places lots of businesses miss. So, whether you're trying to nail down your organisational structure, free employees to work remotely or anything in between, you can do it confidently and in the knowledge that your cybersecurity budget is working for all areas of your business.

Want to find out more about Cyberfort gap analysis? Discover more ways we can help make sure nothing gets past you by visiting: cyberfortgroup.com

CYBERFORT

Get in touch to find out more

Ash Radar Station
Marshborough Road
Sandwich
Kent
CT13 0PL

E: info@cyberfortgroup.com
T: 01304 814800