CYBERFORT

Nothing gets past you with Cyberfort

Here are the smartest answers to some of your colleagues’ most common cybersecurity questions

Start with some questions of your own

Nobody knows what they don’t know. It’s why, when colleagues come to you with questions about cybersecurity policy or best practice, the simplest solution is usually to give them the shortest answer. But could your colleagues and their questions be trying to tell you something?

Knowledge gaps in your business can reveal gaps in its defences. A short answer may help you close the knowledge gap. But closing the cybersecurity strategy gap will take a little more. To make sure nothing gets past you, your colleagues or your organisation, you’re going to need to ask some questions of your own.

In this guide, join us as we review some of the most common cybersecurity questions you face. We’ll show you how, by choosing the smartest answer over the shortest one, you’ll be able to identify gaps in your business’s cybersecurity – and find ways to close them.

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**

CYBERFORT

Are we spending our cybersecurity budget most effectively?

How does our cybersecurity stack up against industry standards and peer organisations?

Why is our cybersecurity insurance policy suddenly so expensive – did we do something wrong?

Turn short answers into smarter ones

So, how do you make sure nothing gets past you? If you're asking that question, you're already on the right track.

Staying sharp isn't just about filling knowledge gaps with the shortest possible answers. Let's take a look at some of the questions you might get from colleagues about your business's cybersecurity and how, if you want to reveal the cybersecurity gaps underneath, the smartest answer will include one or two questions of your own.

CYBERFORT

WHY IS OUR CYBERSECURITY INSURANCE POLICY SUDDENLY SO EXPENSIVE – DID WE DO SOMETHING WRONG?

Shortest answer:

Cybersecurity insurance premiums increased by an average of 28% between the fourth quarter of 2021 and the first quarter of 2022. For the most part, they've not dropped since.

Smartest answer:

Cybersecurity insurance premiums increased because providers expect a greater standard of cybersecurity from their clients. Remember that insurance is not a first line of defence – that responsibility lies with measures like multi-factor authentication, automatic updates and employee training. These controls give providers the assurance they need to cover you at a cost-effective rate. So, do you know what your provider expects? Are you meeting those requirements?

[1] CNBC. 2022. Rising premiums, more restricted cyber insurance coverage poses big risk for companies. Available at: https://www.cnbc.com/2022/10/11/companies-are-finding-it-harder-to-get-cyber-insurance-.html. [Accessed 18 January 2023].

HOW DO OUR CYBERSECURITY STRATEGY AND CONTROL CAPABILITIES STACK UP AGAINST INDUSTRY STANDARDS AND PEER ORGANISATIONS?

Shortest answer:

82% of boards or senior management in UK businesses rank cybersecurity as a high priority – making cybersecurity maturity a source of competition in almost every industry.

Smartest answer:

So, cybersecurity maturity is a point of pride industry wide. But how do you measure yours? To begin with, make sure you're ticking off the basics – risk assessment and risk treatment, a full inventory of your assets and the controls you have in place to protect them. And your competitors? The truth is that competition over cybersecurity maturity can distract you from what's most important. The key to a successful cybersecurity strategy isn't in copying others – it's in understanding your own activities, requirements and capabilities and plotting your own path.

[2] GOV.UK. 2022. Cyber Security Breaches Survey 2022 - GOV.UK.
Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022. [Accessed 18 January 2023].

WE WORK WITH A NUMBER OF THIRD-PARTY SUPPLIERS ACROSS OUR ORGANISATION – ARE THEY BOUND BY OUR CYBERSECURITY STANDARDS, TOO?

Shortest answer:

Organisations that take cybersecurity seriously hold partners and suppliers to the same standards – tracking and measuring third-party strategies in line with their own.

Smartest answer:

Gartner predicts that, by 2025, three out of five businesses will use cybersecurity risk as the main consideration when working with partners or suppliers. Are you doing enough to track your partners' cybersecurity measures? It's not enough to keep a spreadsheet. You need the right to audit their practices and measure their compliance on a regular basis and, most likely, allow them the same privilege.

[3] krontech.com. 2023. Gartner's 8 Cybersecurity Predictions for 2023-2025 | Kron. Available at: https://krontech.com/gartners-8-cybersecurity-predictions-for-2023-2025. [Accessed 18 January 2023].

WE’VE GOT BUDGET TO MATURE OUR CYBERSECURITY PROGRAMME – BUT ARE WE SPENDING IT EFFECTIVELY?

Shortest answer:
Nearly half of organisations say they have what they consider to be a problematic shortage of cybersecurity skills – and no choice but to spend budget to make up the shortfall.

Smartest answer:
This skills shortage points to the complex and ever-evolving nature of cyber threats – and the need for organisations to continually adapt and enhance their responses. It can be tempting to dedicate the majority of your budget to information security and risk management products that protect your systems, data and reputation. But are you really addressing the issues? What happens when the landscape inevitably evolves? Effective use of budget balances investments in technology with investments in personnel – in the development and cybersecurity training of your employees – for a more robust and resilient cybersecurity posture.

[4] Enterprise Strategy Group, a division of TechTarget. 2023. 2023 Technology Spending Intentions Survey | Enterprise Strategy Group. Available at: https://www.esg-global.com/2023-technology-spending?utm_campaign=ESG%20Research&utm_source=slider. [Accessed 09 February 2023].

Make sure nothing gets past you

The smartest answers aren’t always the shortest ones. When it comes to your cybersecurity, it’s not enough to fill a knowledge gap – you have to go further to identify and fill the corresponding gap in your strategy.

From your business’s approach to remote working to your customers’ regard for your cybersecurity (and everything in between), you’ll find the smartest answers to your colleagues’ cybersecurity questions have something in common. They review your current position against what you need to do to be compliant – making sure you align to your business objectives and account for appetite for risk exposure – to make sure your strategy is fit for purpose. Cyberfort can help, too. This is exactly the approach we take to gap analysis, turning good questions into great cybersecurity outcomes.

Want to find out more about Cyberfort gap analysis? How about get the smartest answers to even more of your colleagues’ cybersecurity questions? 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