Cebr
Making Business Sense

CGI
Experience the Commitment®

Cyber security in the boardroom:

UK plc at risk

BUILDING ON 40 YEARS OF COMMITMENT

Contents

Methodology

CGI UK commissioned and directed the Centre for Economics & Business Research (Cebr) in partnership with Opinium Research to survey 150 C-level and boardroom business leaders from the UK's largest companies (1,000+ employees). The research excluded consideration of government decision making on cyber security because of its substantially different approach. Primary research was carried out over a two month period from December 2015 to January 2016.

The data was then subjected to sophisticated economic modelling by Cebr to identify the relative risk profile for industry sectors.

Foreword

Cyber security isn't a new issue. At CGI we've been helping to protect the UK's critical national infrastructure, government and some of the country's largest companies for over 40 years – since the outset of computing. However, what certainly is new is the rapidly growing business dependence on networked systems and the Internet, coupled with the rapidly evolving cyber security threat landscape and the amount that is at stake for companies in today's digital-first world.

As companies focus on digitising every area of their operations from the supply-chain, to the back-office, to customer interaction, the potential for a cyber security breach grows exponentially. That's why cyber security is 'part of everything we do' at CGI, and capabilities are baked into our teams delivering digital transformation and change at every level.

Recognising cyber security as a risk is one thing, acting on it turns out to be quite another. We often find that business leaders are worried about cyber security but are less sure about how to act on it. That's why we commissioned this significant research analysis from the Centre for Economic and Business Research. It provides valuable insights and explanations that start to address this particular challenge.

The findings contained within this report focus primarily on a question which receives relatively little attention, 'can boards effectively govern cyber security?' This question is of such relevance because the board's perspective and sponsorship of an issue so often sets the tone for how seriously and effectively a company approaches it. Cyber security as we know it today is one of the newest risk boards have been faced with. Boards are responding in a variety of different ways, from locking down systems to the point of unusability, to laying off the risk to insurers, a strategy that is evidenced by the rapid growth of cyber insurance products. Today, the management of such risks is poorly understood by the majority of decision makers.

With this study we wanted to investigate how well boardrooms at major UK companies are equipped to deal with the growing threats posed by cyber attacks and also to identify which sectors of the UK economy carry the greatest cyber security risk. We also aim to encourage a debate about how boards can take positive steps to improve levels of governance as a means of reducing the UK's exposure to cyber risks.

To that end I encourage you to share your perspectives of the findings herein either directly with me, via your CGI contacts or indeed via social media.

Dr Andrew Rogoyski
Vice President Cyber Security Services, CGI UK

UK plc faces up to cyber risk

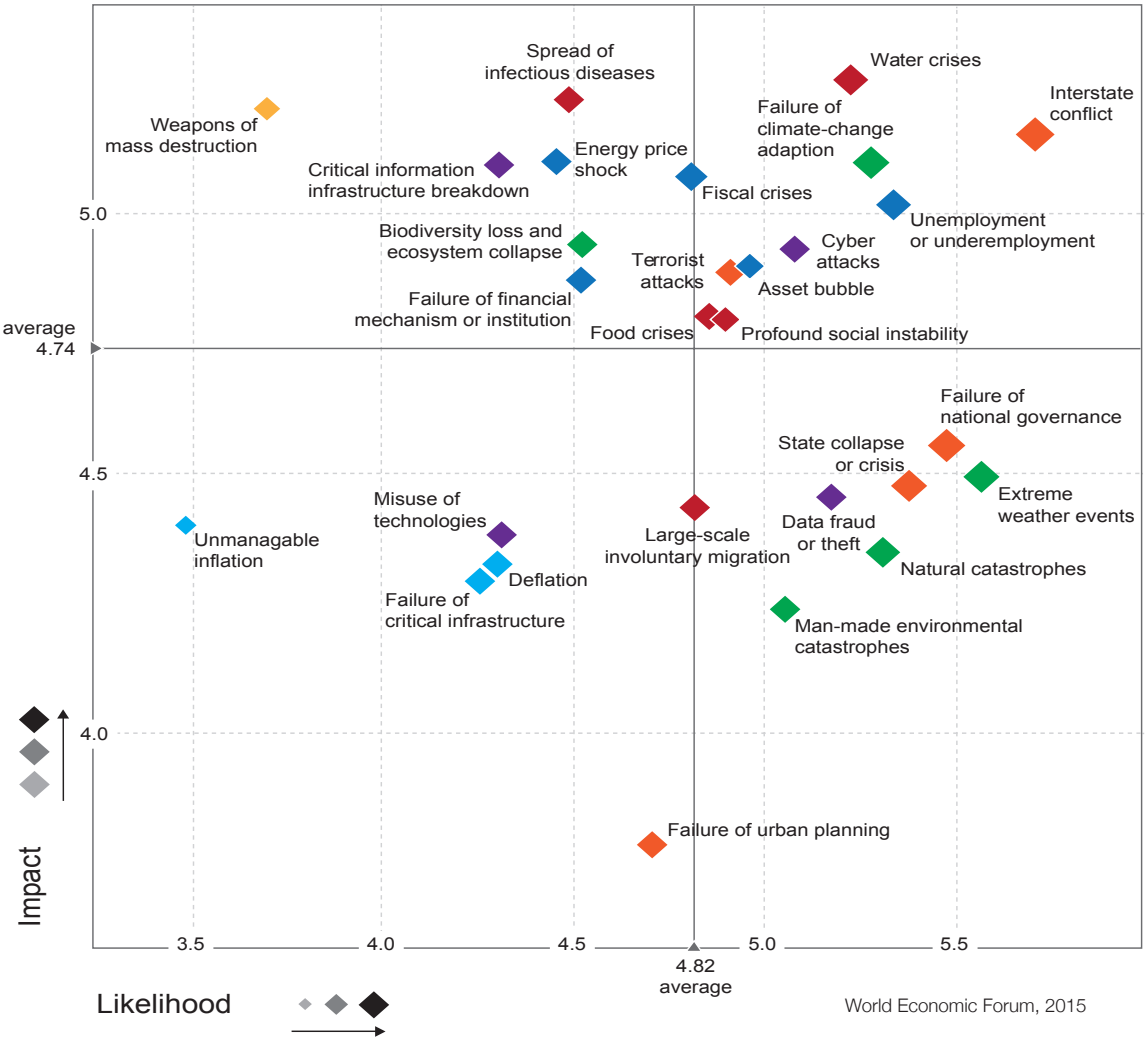
2015 saw cyber crime and data security risks elbow their way to the top of UK plc's boardroom agenda.

In recent years a raft of studies by security agencies, consultants and governments painted a vivid picture of the likelihood and impact of data security breaches on global business and economic life. The World Economic Forum warned that cyber attack is one of the top risks facing the world today. Looking closer to home, AON[1] identified the UK as above the global average for cybercrime vulnerability although earlier work showed the UK was ahead of other nations when combining factors such as education, adoption of Internet services and business culture[2]. More recently, the 2015 Global Cybersecurity Index[3] ranked the UK behind the United States, Canada and Australia on cyber risk preparedness.

But it seems it took the arrival of cyber attacks in the headlines to crystallise the issue. October's TalkTalk breach in particular appears to have woken UK plc to the growing risks presented by cyber security breaches. Over four out of five (81%) of executives surveyed for cyber security in the boardroom say that high-profile cyber breaches like TalkTalk led to greater awareness and scrutiny of cyber risk by boards.

1. "Exploring the latest cyber risk trends in EMEA", 2014
2. "Cyber Power Index" Booz Allen Hamilton and the Economist Intellihgence Unit, 2011
3. ABI Research, "Global Cybersecurity Index", 2015

World Economic Forum top global risks, by likelihood and impact.
Identified as one of the biggest risks facing global business, the threat of cyber attack also poses particular challenges to UK business.



TalkTalk: costs of cyber attack add up

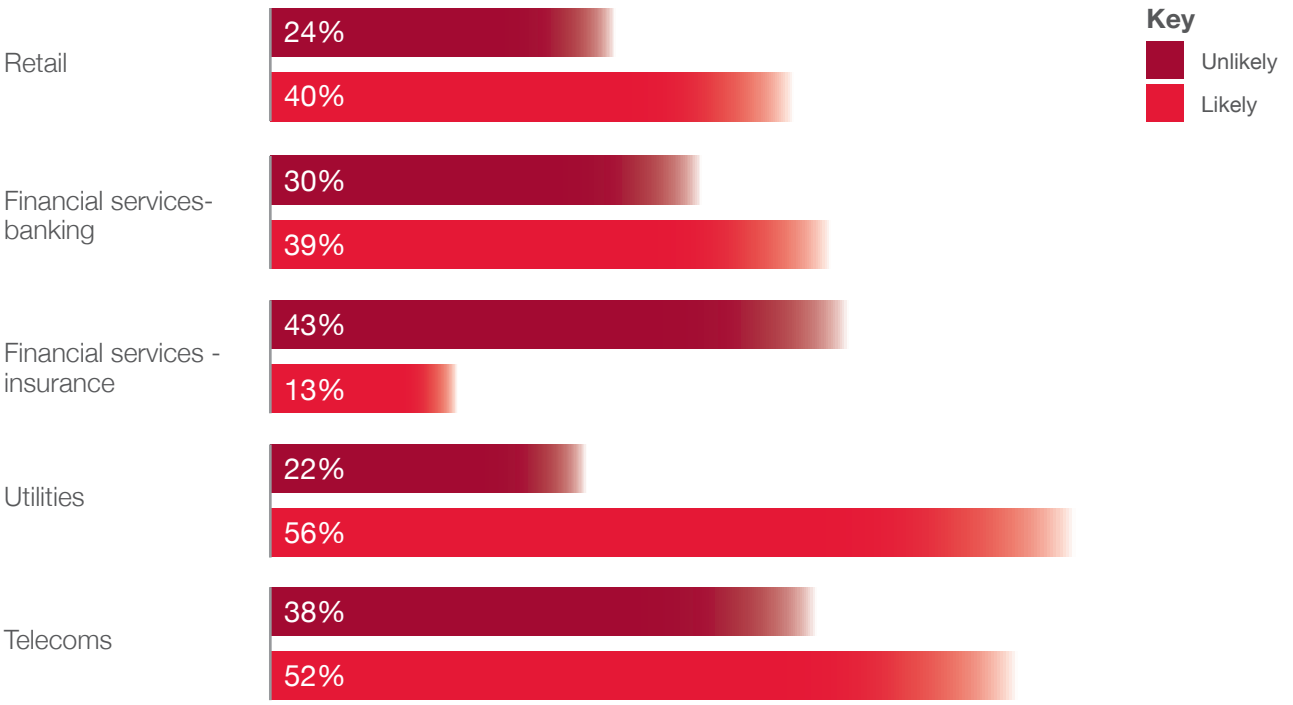
In October 2015, the UK telecoms and media company TalkTalk revealed that it had suffered a massive cyber attack. Largely played out in public, the TalkTalk hack was headline news for weeks, with the challenging nature of the incident damaging confidence in the brand and the company's leadership. By the time the dust had settled, the company was reported to have shed over 100,000 customers and racked up costs of £60 million[4]. At one point, thirty per cent was wiped from the value of TalkTalk shares, however TalkTalk has recovered well from this challenge, becoming an advocate of increased transparency of cyber breaches to highlight the need for improved security across UK companies. The incident demonstrates that no matter how competent the company or its leader, cyber security risk is large both in terms of likelihood and severity.

[4] TalkTalk counts the cost of cyber-attack. The Guardian, 2 February 2016. http://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave

A clear and present danger

For UK boardrooms cyber security breaches are not an abstract concept: well over a third (38%) of board members think it likely that their company will experience a cyber security breach at some point in the next twelve months.

Figure 1: C-level views on how likely it is that their company will suffer a cyber breach in the next 12 months

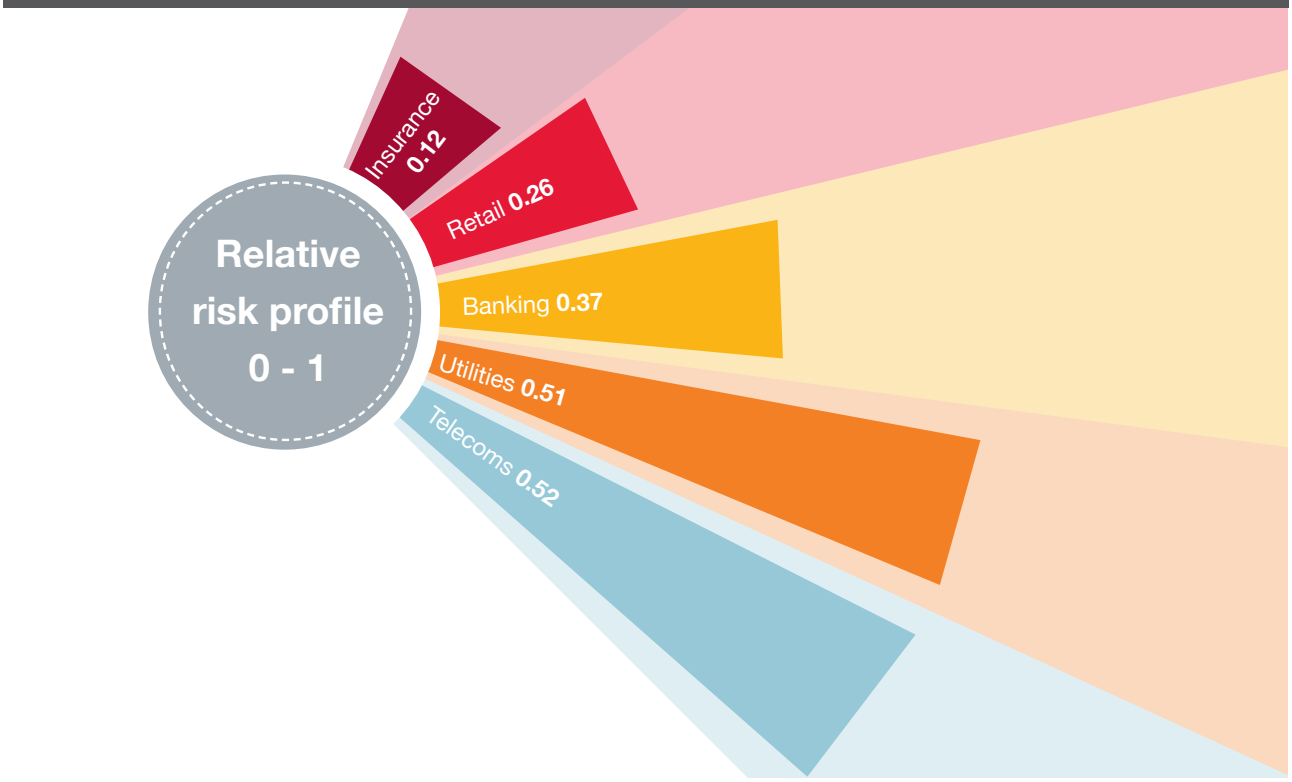


Of the five sectors featured in the survey, executives in telecoms and utilities sectors are especially pessimistic. Over half (52%) of business leaders in telecoms - and 56 per cent in utilities - think their IT system security may be compromised within the year.

Modelling of the survey data carried out by Cebr reveals that these sectors have a particularly poor risk profile, relative to the retail, financial services (banking) and financial services (insurance) sectors. In terms of cyber security preparedness, telecoms and utilities can be regarded as more at risk than other sectors. This paper will include special focus on telecoms and utilities, as they present valuable lessons for any organisations intent on rapidly improving cyber risk resilience.

The econometric model uses a combination of perceptions of the nature of sensitive information stored, the value of such data, the expenditure on defending against attacks and the overall awareness of risk to the company and sector to derive an objective risk rating.

Figure 2: Relative risk profile for key sectors of the UK economy, scale between 0 (low) and 1 (high).



Telecoms and utilities at risk

Perhaps reflecting a loss of confidence following recent high profile incidents, telecoms sees itself lagging other sectors with the lowest level of boardroom cyber security expertise. Just 29 per cent of telecoms boards are viewed as having a high degree of expertise, whilst firms in this sector hold sensitive data with an average estimated value to each company of over £42 million.

Telecoms respondents were also most pessimistic; with over half (52%) believing their company was likely to experience a significant breach during 2016. Perhaps in response, 76% of boards in the telecoms sector plan to increase their use of external cyber security expertise and the sector plans to increase investment in cyber security technology and personnel by 12% this year, compared to 9% in retail and 7% in insurance.

The utilities industry is also at risk, with boards discussing cyber security least often - at 40 per cent of utilities firms the issue makes the boardroom agenda just twice each year. Companies in the sector hold sensitive data estimated at over £50 million on average but were found to be significantly behind other sectors in terms of having robust plans in place to handle a cyber event, with just 1 in 5 boards confirming their firm's cyber crisis management plan is well developed. This is surprising given that utilities firms have a culture of high resilience with good business continuity planning, perhaps showing a lack of maturity in the treatment of cyber security as a major business risk. Utilities firms plan to increase cyber investment by 14 per cent, and over 90 per cent of boards plan to look to external consultants to support their plans.

Identifying the cyber risk impacts

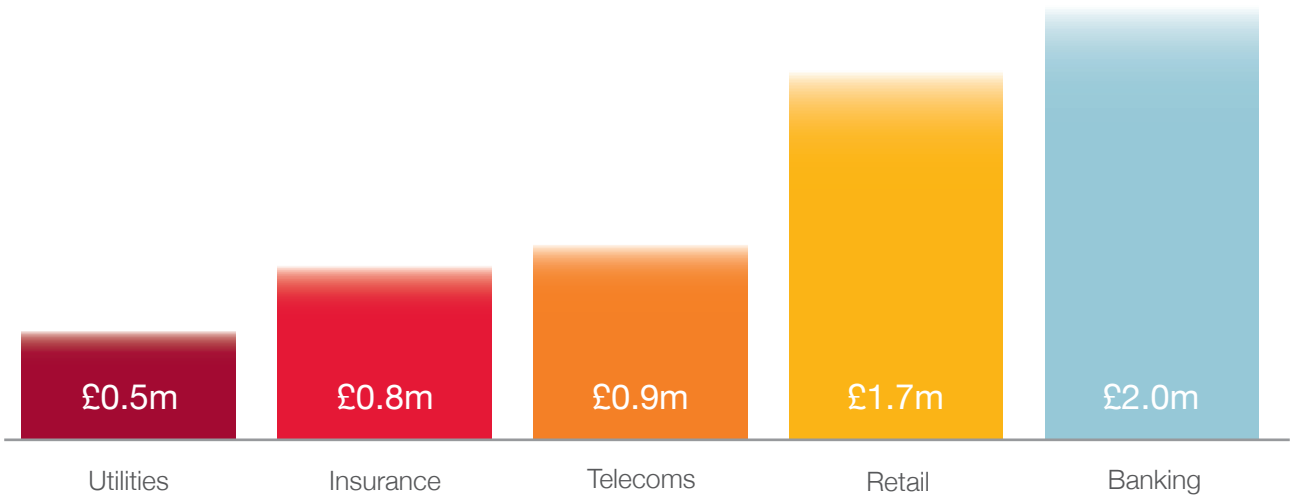
UK boards are subjecting cyber risks to greater scrutiny - but what specific threats are on the boardroom radar?

The increasingly pervasive use of digital technologies in today's corporations to manage everything from customer interactions to operations means that a cyber breach can have very different consequences in different companies, and the varied profile of cyber damage reflects this.

In financial terms alone, the stakes are high. On average, the UK companies that participated in the survey hold £52.4 million of sensitive information each, including Intellectual Property or other commercially valuable data. Among financial services (banking) firms, this figure rises to £64.8 million.

UK business leaders estimate significant 'hard' cost impacts of up to £2 million associated with the loss or corruption of their most valuable data in any given year. If the cost of cyber breaches trend continues to rise at its current rate (the cost of cyber attack for large UK firms was thirteen times higher in 2015 than in 2012)[5] these cost impacts are likely to ramp up substantially.

Figure 3: Average annual total cost of loss or corruption of most valuable data

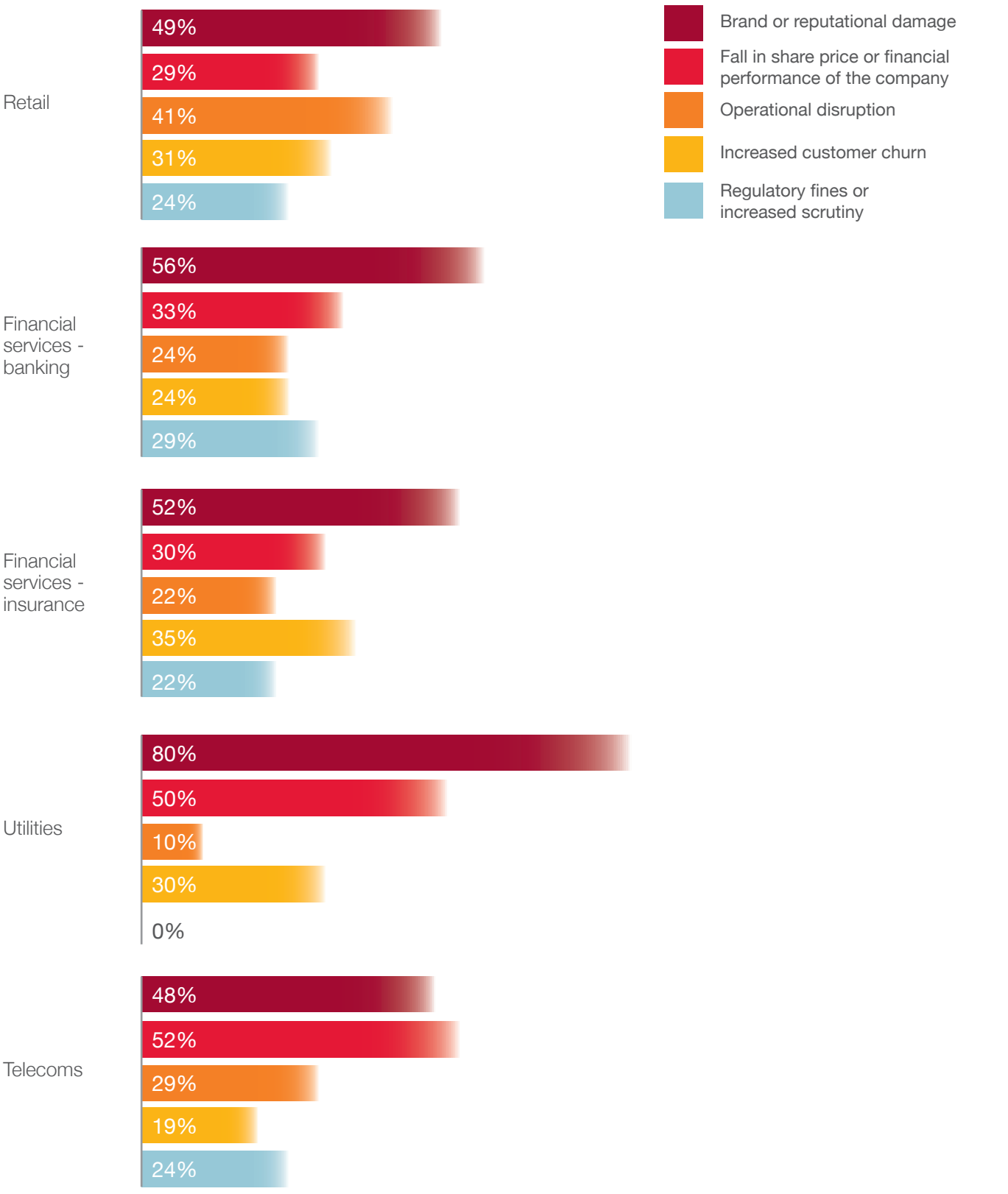


However, while the cash impacts are significant, the survey data shows that UK plc is more concerned by the reputational impact of a data breach. Brand damage is identified as the number one impact by leaders in every sector, apart from telecoms. Here, and possibly with memories of TalkTalk fresh in telecoms executives' minds, the chief impact is seen as damage to the share price or financial performance.

A significant proportion (41%) of retail executives identify operational disruption as a concern, perhaps reflecting the degree to which cyber security-related problems can threaten trust, impair the customer experience and disrupt e-commerce.

[5] Information security breaches survey. HM Government (BIS) and PwC. 2015

Figure 4: C-level perspective on the greatest impact of a cyber security breach to their organisation



If an attacker can gain access to your IT systems, your digital infrastructure, there are many ways in which they can do harm to your organisation.

Consider the following consequences of an attack:

- Data breach – Sensitive information is lost or leaked, including personal information covered by the Data Protection Act or material that is confidential to your organisation
- Intellectual property theft - Theft of critical knowledge and know-how such as designs, trade secrets and market sensitive data such as corporate strategy or acquisition plans
- Disruption to services – Causing your own or 3rd party online services to be unavailable for a period of time
- Reputational damage – Revealing information that could have a long-term impact on your own reputation or that of a 3rd party, including customers and suppliers
- Malware transmission – You cause damage to a 3rd party by inadvertently passing on malware
- Extortion – Data is encrypted and inaccessible unless payments are made to the attacker
- Blackmail – Data which an attacker threatens to expose unless a payment is made to them
- Espionage – Gaining government or commercial secrets, not necessarily owned by your organisation
- Sabotage – Deliberate damage to your organisation's operations
- Embarrassment – Revealing data that could embarrass your staff, your organisation, or 3rd parties
- Internal reputation – Exposing material which causes your own employees to doubt the standing of your organisation

Are you convinced that your organisation is sufficiently prepared to deter, detect or respond to an attacker that could do damage in any of these ways?

Most information of value is now held digitally, whether as emails, databases, documents, or any number of other forms.

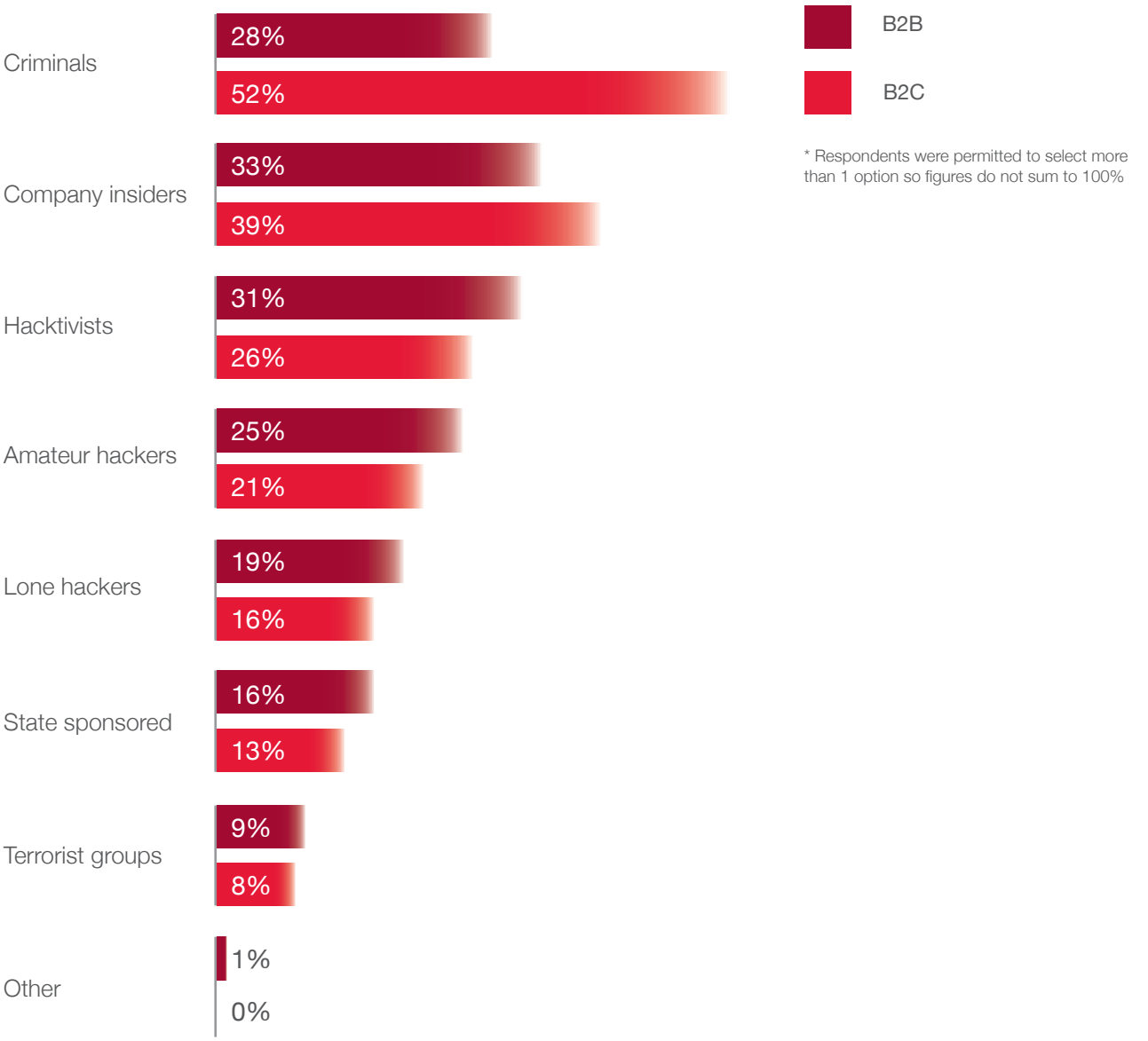
Such digital information needs to be protected. When considering what type of information is important to you and your organisation, focus on material that underpins your commercial advantage. Then consider what would happen if such information fell into the wrong hands. For example:

- Business Assets – Strategies, plans, acquisition targets and major bids
- Personal information – Customers, employees, Big Data repositories such as customer buying behaviours, financial information, including credit card details
- Communications – Digital communications such as email, documents, messages and videos, including personal and private communications
- Designs – Current and future designs, including patents
- Sales data – Details of customers, contact details, insights, behaviours, past purchases and future purchase plans
- Digital Product – Software, videos, audio, designs, analysis, books and other forms of digital content
- Software – Trading algorithms, pricing models and market analysis
- Processes – Key business processes, including those unique to the organisation
- Contracts – With customers, suppliers and partners
- IT information – Network designs, security measures, IT assets, employee credentials, supplier and partner credentials
- Facilities – Company locations, access controls, personnel, plant design, equipment design, maps, future plans and costs

If your business has any of the above, do you know where it is kept and whether you have the security in place to keep it safe?

Asked to identify the most likely origins of an attack, executives are most concerned about the risk posed by criminal gangs, company insiders and hacktivists (those seeking to make a political point via a hack). Of course, knowing who your attackers are likely to be and what they might be interested in doing, can significantly change a company's plans to secure their enterprise.

Figure 5: C-level perspective on who or what is of most concern in terms of causing harm



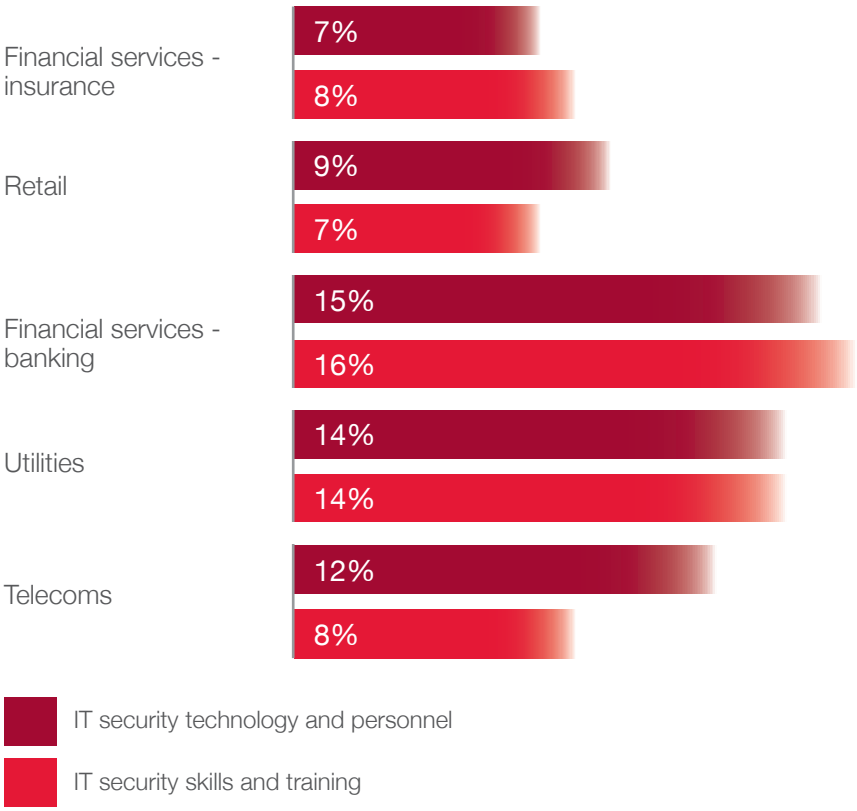
Mitigation strategies

UK boardrooms have a growing awareness of the urgency and extent of cyber risk. Here, cyber security in the boardroom asks what strategies they are putting in place to manage this risk. One increasingly popular strategy is to insure against the risk.

While insurance offers a first port-of-call approach for reducing the impact of risks, the research suggests senior leaders have low levels of confidence in the ability of standard business insurance policies to offer comprehensive protection. Among B2C sector companies – such as retailers – over two thirds (70%) of board members believe standard business insurance only partially covers cyber-related risks. The picture is slightly better in the B2B sector, where just over half (58%) believe they have partial cover. In reality, the scope of business insurance cover is changing, with many products starting to include exclusions against claims caused by cyber incidents, accompanied by rapid growth in specialist cyber security insurance products.

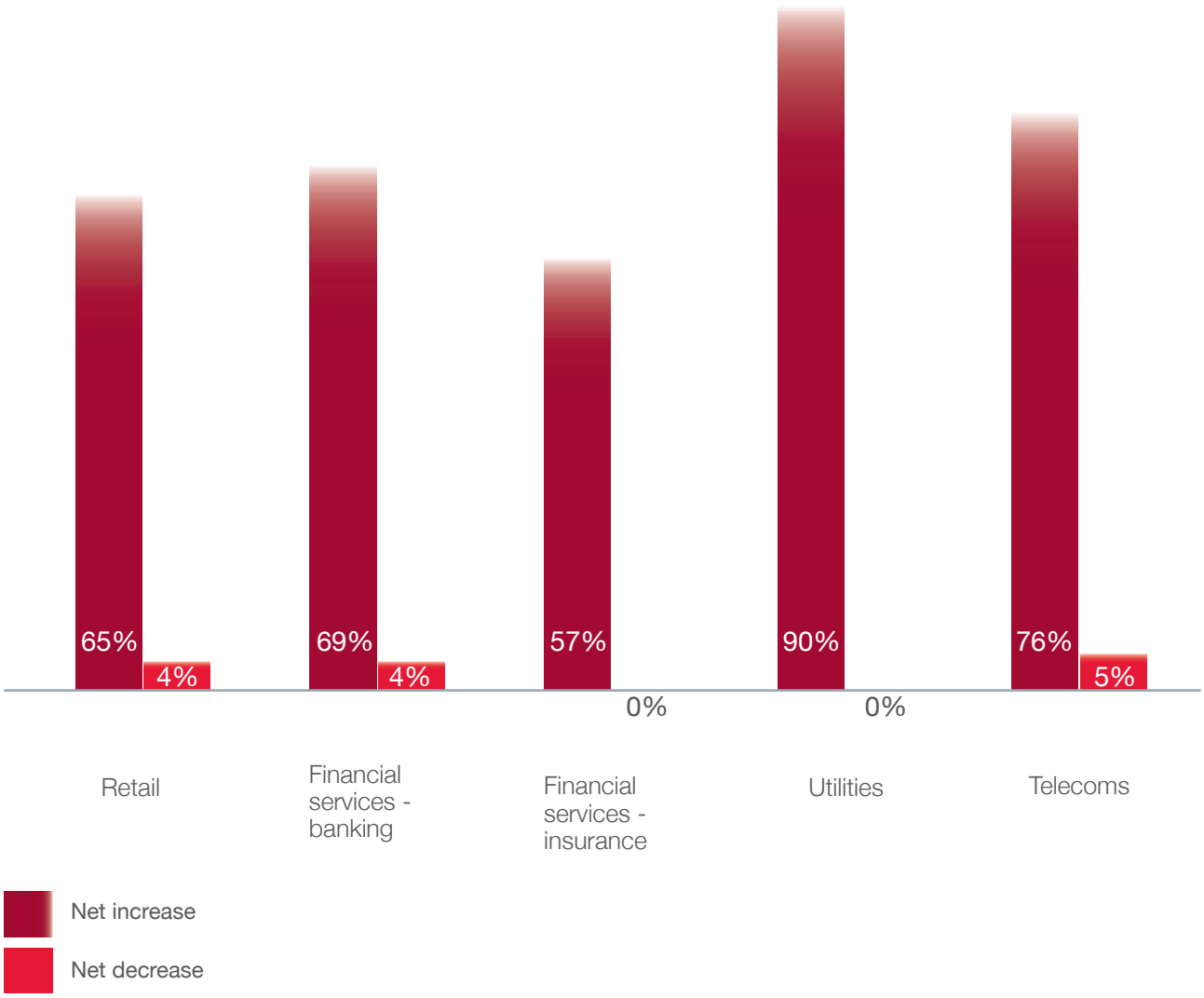
It appears UK plc puts more faith in IT investment as a strategy for mitigating data security risks. Today, cyber security accounts, on average, for 9 per cent of IT spend, including training staff and updating IT systems. Looking ahead, board members expect this spend to rise by 11 per cent on average. In financial services (banking), investment in IT security is expected to grow by as much as 16 per cent.

Figure 6: C-level view of planned increases in cyber security investment levels over the next 12 months



Boardrooms will also increase their reliance on third party experts to help them deal with cyber risk. Today, less than half of boards are confident in the cyber security advice they receive. On average, companies source only 15 per cent of their cyber expertise externally. However, this figure is set to rise as over two thirds (68%) intend to bring in more external expertise to help mitigate cyber risk. Among companies in sectors identified as high risk relative to industry as a whole, the demand for outside expertise is particularly marked. Nine in ten (90%) of utilities companies and over three quarters (76%) of telecoms firms intend to call on third party consultants.

Figure 7: C-level perspectives on intended increase or decrease of externally sourced cyber security expertise



The challenge to boardrooms

UK boards understand that cyber security breaches threaten their ability to do business – but the research data suggests they need to do more to equip themselves to manage these risks.

The central role of the company board in driving the business, setting strategy and overseeing operational performance is fundamental. In this section cyber security in the boardroom looks in detail at issues around governance and how these impact a company's cyber security preparedness.

The research shows that UK boards are paying more attention to cyber security in the wake of high-profile cyber breaches like TalkTalk with 81 per cent confirming such incidents have heightened scrutiny. But it is not clear that this has yet translated into a regular formal process: while almost half (48%) of boards discuss cyber security every few months on average, just a third review their organisation's level of 'acceptable' IT security risk on a monthly basis.

The persistence of attitudes that regard data security as an IT matter may explain why most boards are not regularly reviewing their vulnerabilities: over a quarter (28%) of board members relegate cyber risks to the status of an 'IT issue', rather than a threat to the enterprise as a whole.

Reflecting this relatively low level of formal scrutiny, just over half (53%) of boards have well developed crisis management plans in place. Utilities companies reveal a significantly low level of preparedness: only a fifth (20%) have well developed plans in place. For 10 per cent these plans are 'in development' and not yet implemented. Their level of cyber security preparedness is at odds with their wider crisis management and business continuity planning which, as an industry, is very well developed.

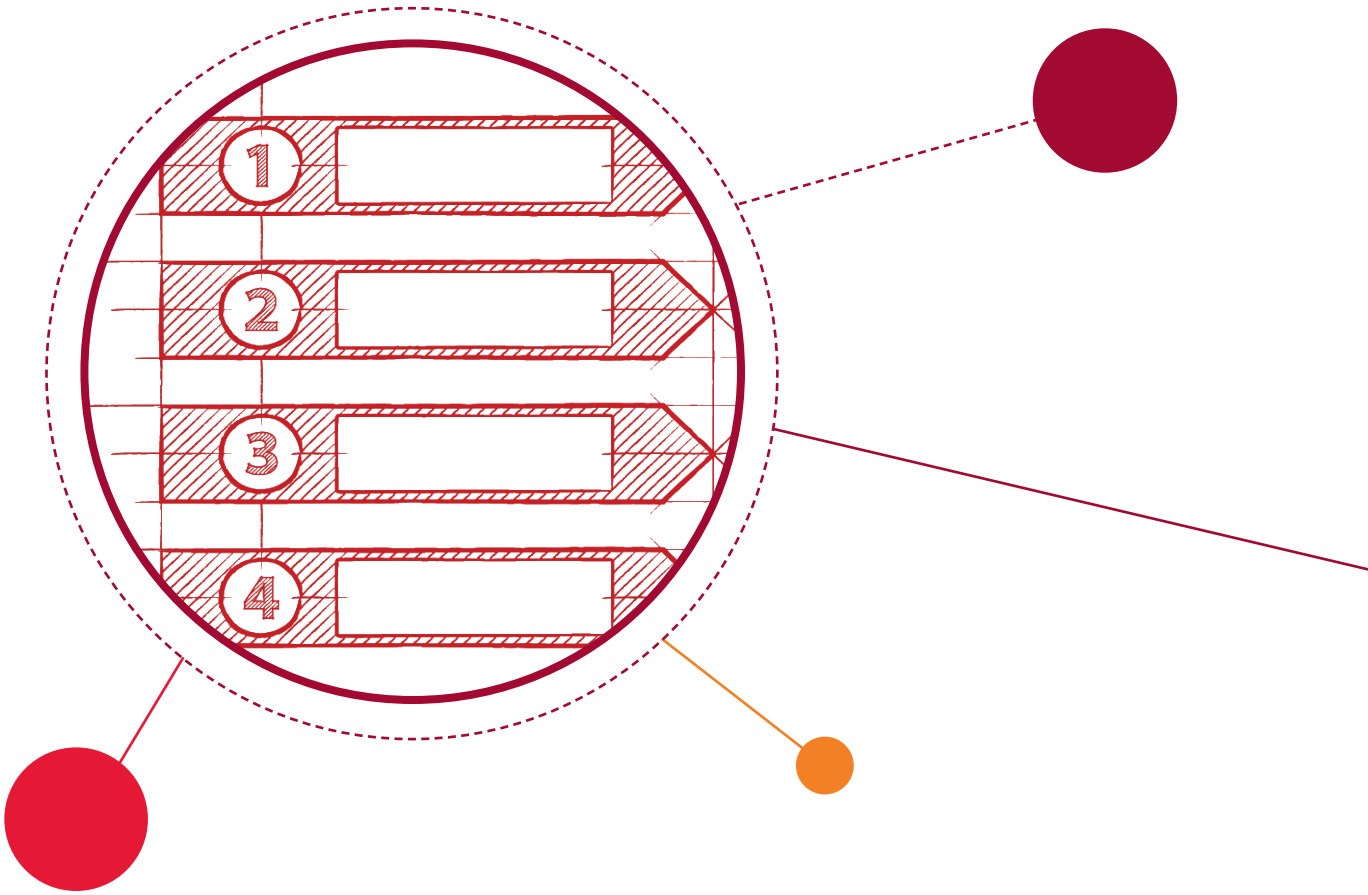
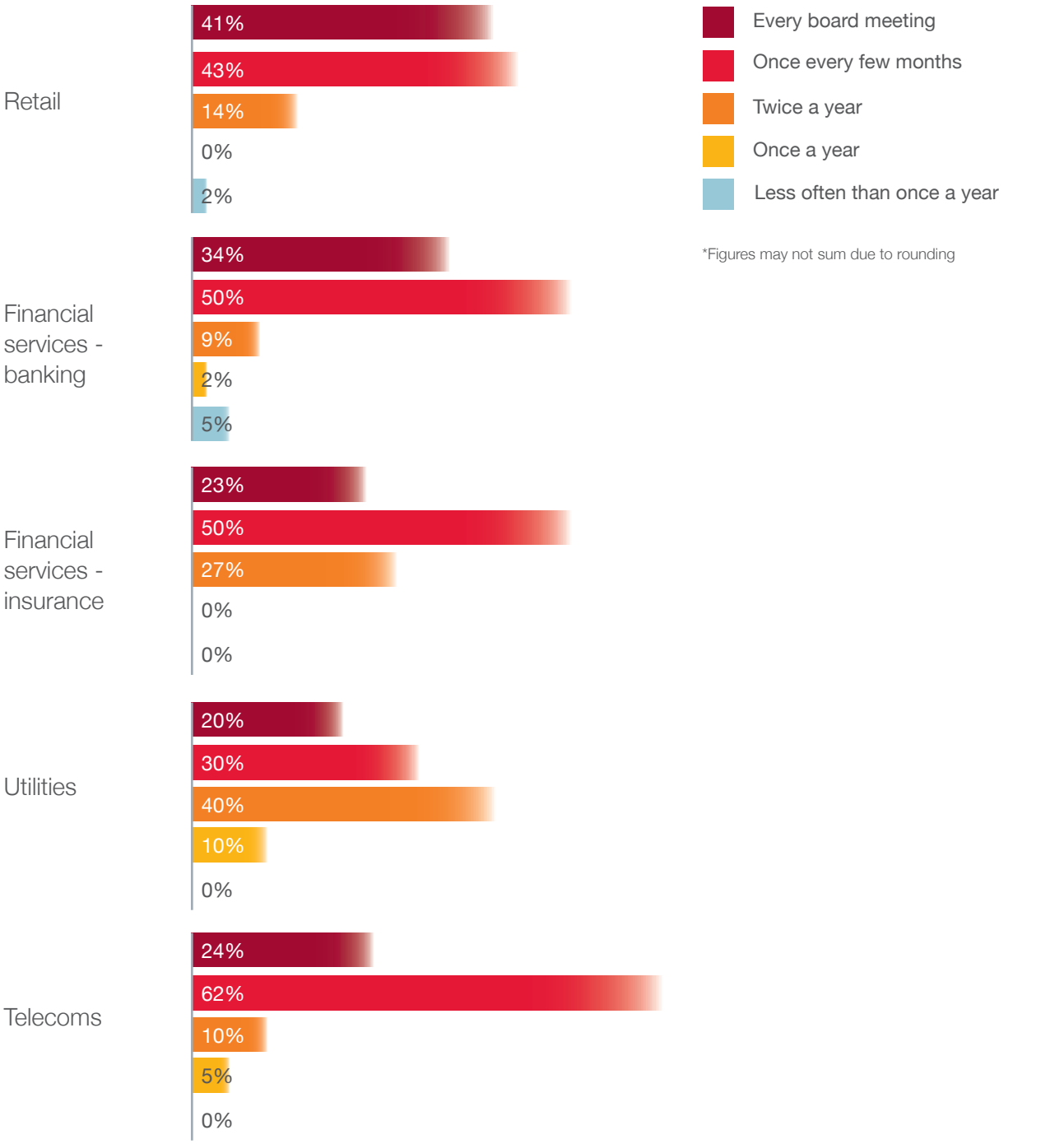


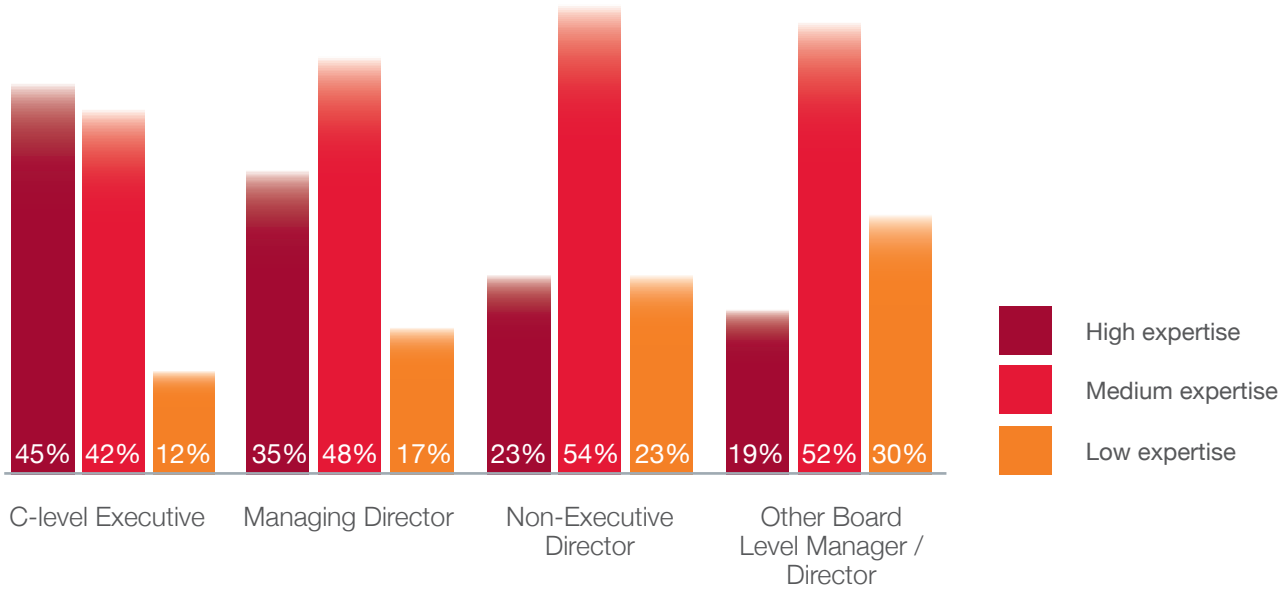
Figure 8: C-level views on how often cyber security is included on the boardroom agenda



Understanding the issues

The cyber security in the boardroom research suggests variable levels of knowledge about cyber risk issues among UK boardroom leaders: just over a third (35%) of the leaders surveyed believe that they have board members with a high-level of cyber security expertise. This is particularly evident in telecoms where only 29% are thought to have a high-level of expertise, perhaps reflecting a loss of confidence following the TalkTalk incident.

Figure 9: C-level views on the degree of cyber security expertise held by their company's board



More questions about knowledge levels emerge when it comes to the regulatory changes that are reshaping cyber security. The forthcoming European General Data Protection Regulation (GDPR) and Network & Information Security Directive will significantly impact the legal and regulatory environment for UK companies, changing penalties for mishandling sensitive data, introducing new definitions of what comprises sensitive data and requiring that larger firms publicly disclose cyber breaches. However, only just over a third (37%) of board members are fully aware of these imminent changes and that number falls to 23% for Non Executive Directors.

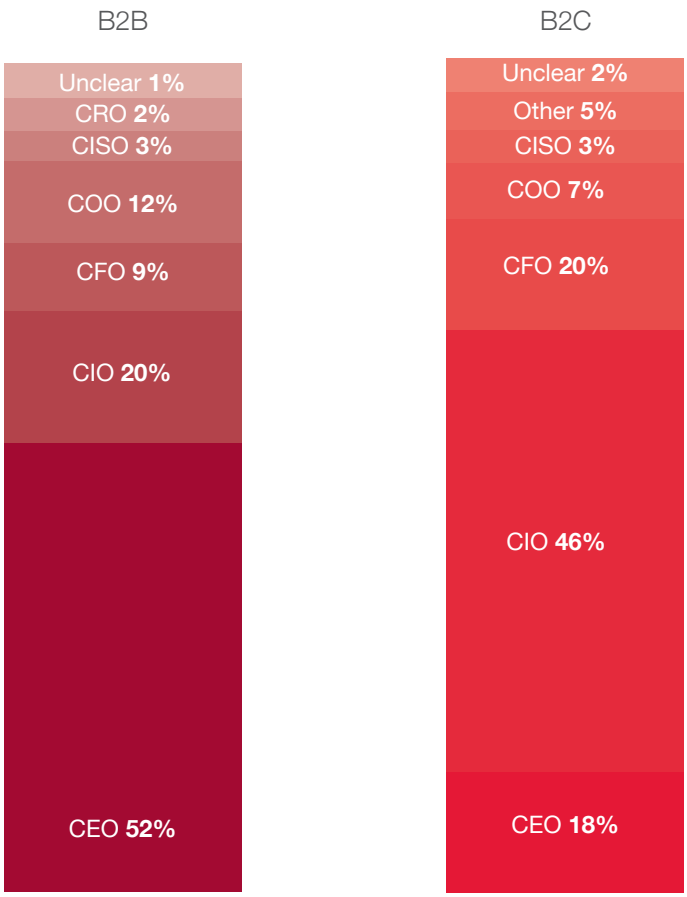
Boardroom roles

Each board role contributes its own set of skills, experience and insight to the board as a whole. The Non-Executive Director (NED) is described by the Institute of Directors as a source of 'constructive challenge' in the boardroom. NEDs often have even greater experience than the management team and they bring this to bear on executive plans to ensure they are robust

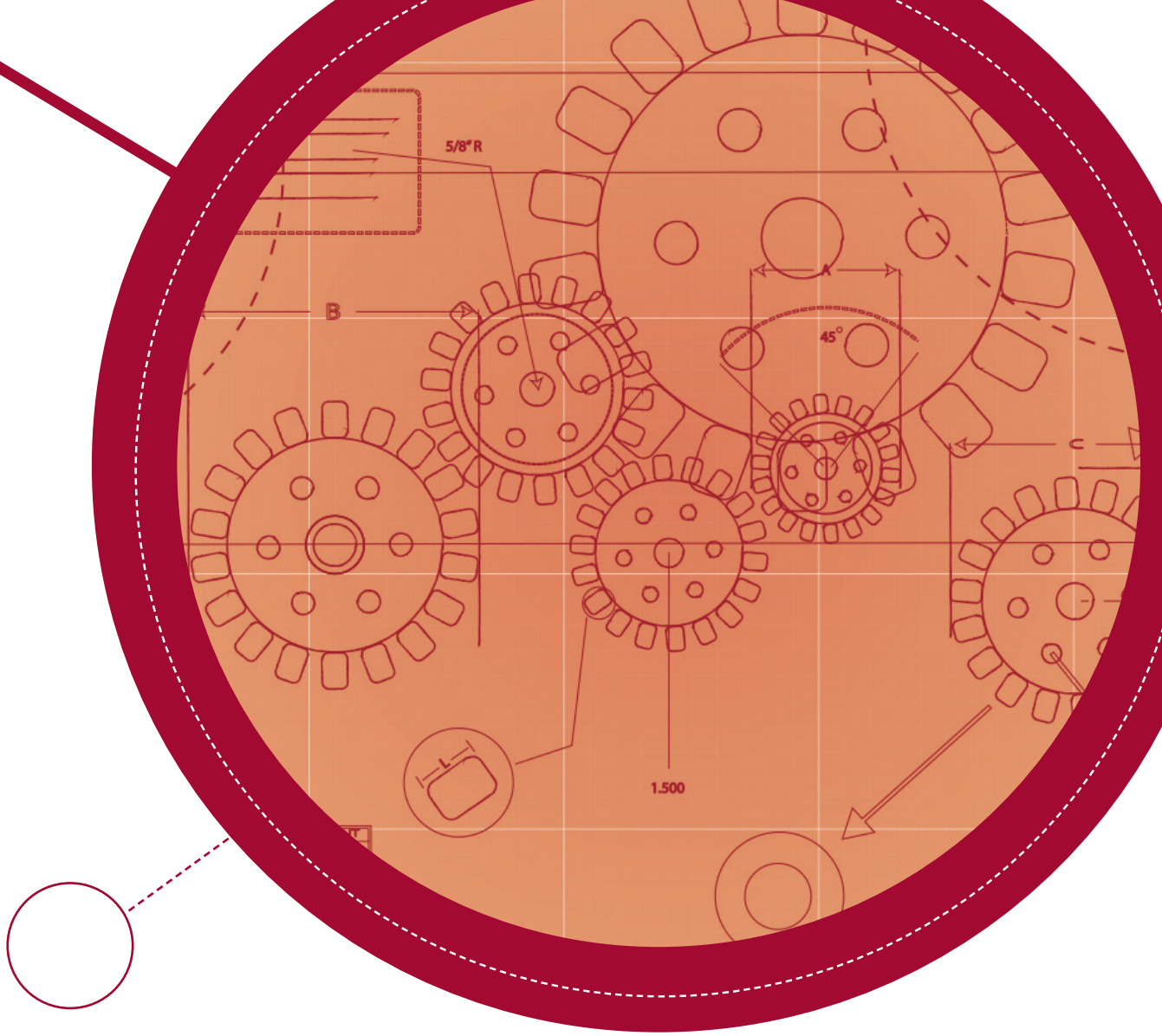
However, where cyber security is concerned, the research suggests NEDs may lack the specific experience and self-confidence to perform this role. Less than a quarter (23%) of NEDs – far lower than the overall average for board members – are thought to have a high-degree of cyber security expertise.

While a significant proportion of boards currently assign ultimate responsibility for cyber security to the CEO (38%) or the CIO (31%), the research finds that specialist Chief Information Security Officers (CISOs), senior security specialists, are only a reality in a small minority (3%) of companies.

Figure 10: C-level perspectives on where board level cyber security accountability resides at their company



* Remaining respondents selected other or reported that responsibility is not clearly assigned, hence not adding to 100%.



Spotlight on the CEO

As the most visible element in a company's leadership, the CEO plays a pivotal role in the development of a cyber risk-ready enterprise.

Among all the boardroom roles, the research finds that CEOs are the most attuned to cyber risk issues. In the wake of the TalkTalk breach, C-level executives are more likely (89 per cent versus 81 per cent for other board level managers/directors) to perceive a shift in the boardroom towards greater scrutiny of data security topics.

CEOs are the board member most likely to carry ultimate responsibility for cyber issues in B2B companies. In contrast, B2C companies tend to assign responsibility for IT security to the CIO. That said, in case of a breach it will be the CEO who will be called upon to face the media.

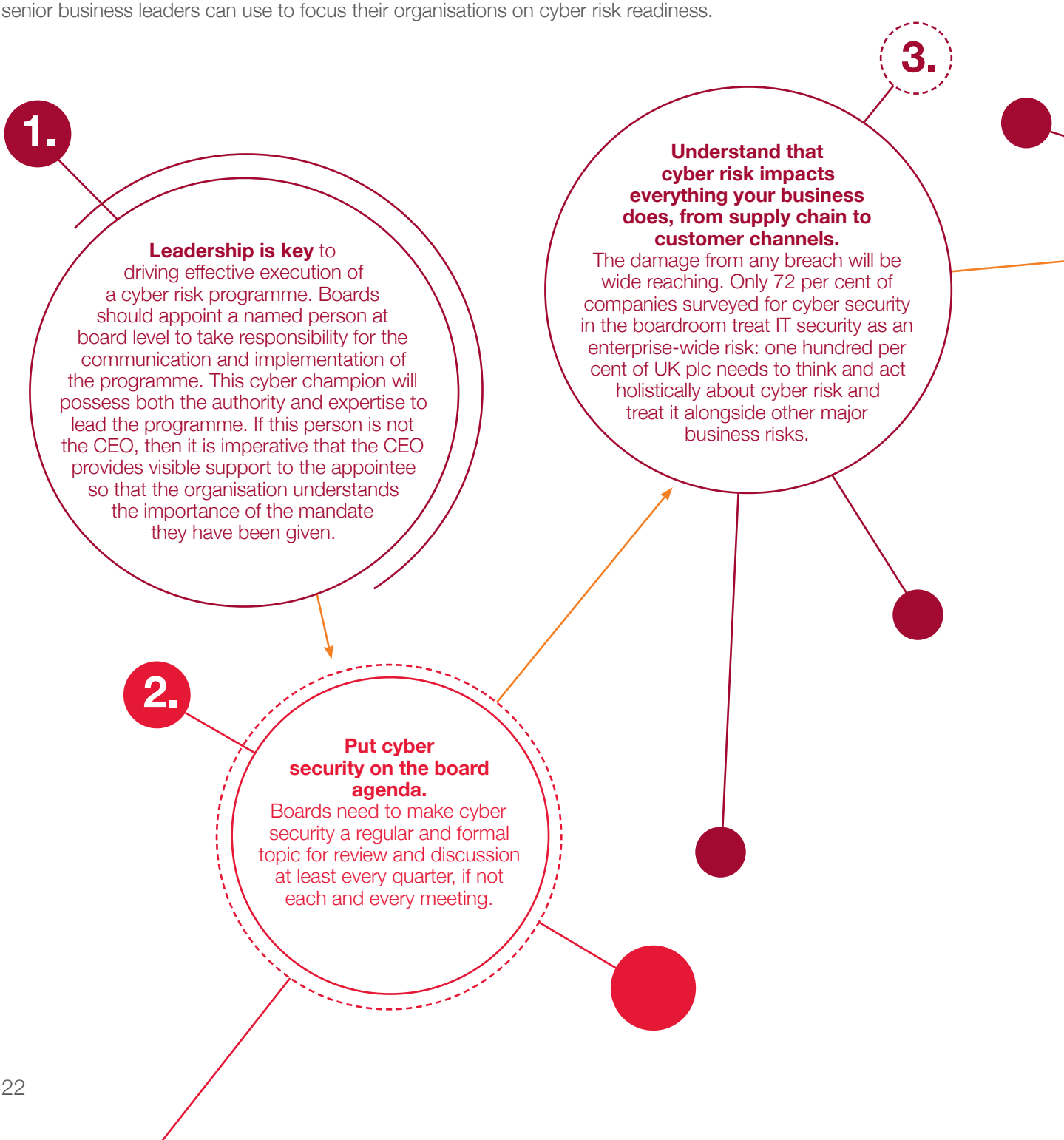
Many CEOs seem bullish about their personal levels of cyber risk competence. Almost half (45%) say that they have a high level of expertise, and a further 42% claim to have a 'medium' level of expertise. To drive effective cyber risk mitigation programmes, CEOs will need to call on and build these reserves of self-confidence and knowledge whilst recognising they must instil a similar focus amongst fellow board directors and colleagues at large.

Seven Steps

Recommendations for how UK boards can implement effective cyber security governance.

The research and analysis undertaken for 'cyber security in the boardroom' reveals high levels of board awareness about the immediacy of cyber security threats. Board leaders clearly appreciate that cyber crime and data security breaches have created a new and growing profile of risks that could impact their operational performance, reputation and profitability. However, it is not apparent that companies have the strategies and execution in place that will allow them to manage these risks most effectively.

Drawing on its experience in helping senior executives address the key governance and leadership issues around cyber threats, CGI's Cyber Security Services team has developed Seven Steps: a set of actions that senior business leaders can use to focus their organisations on cyber risk readiness.



These Seven Steps are the beginning of a process – one that will lead to companies building their understanding, resilience and confidence for managing cyber security risks. To find out more about cyber security risk issues and understand what they mean for your boardroom and business we invite you to continue the dialogue with us here at CGI.

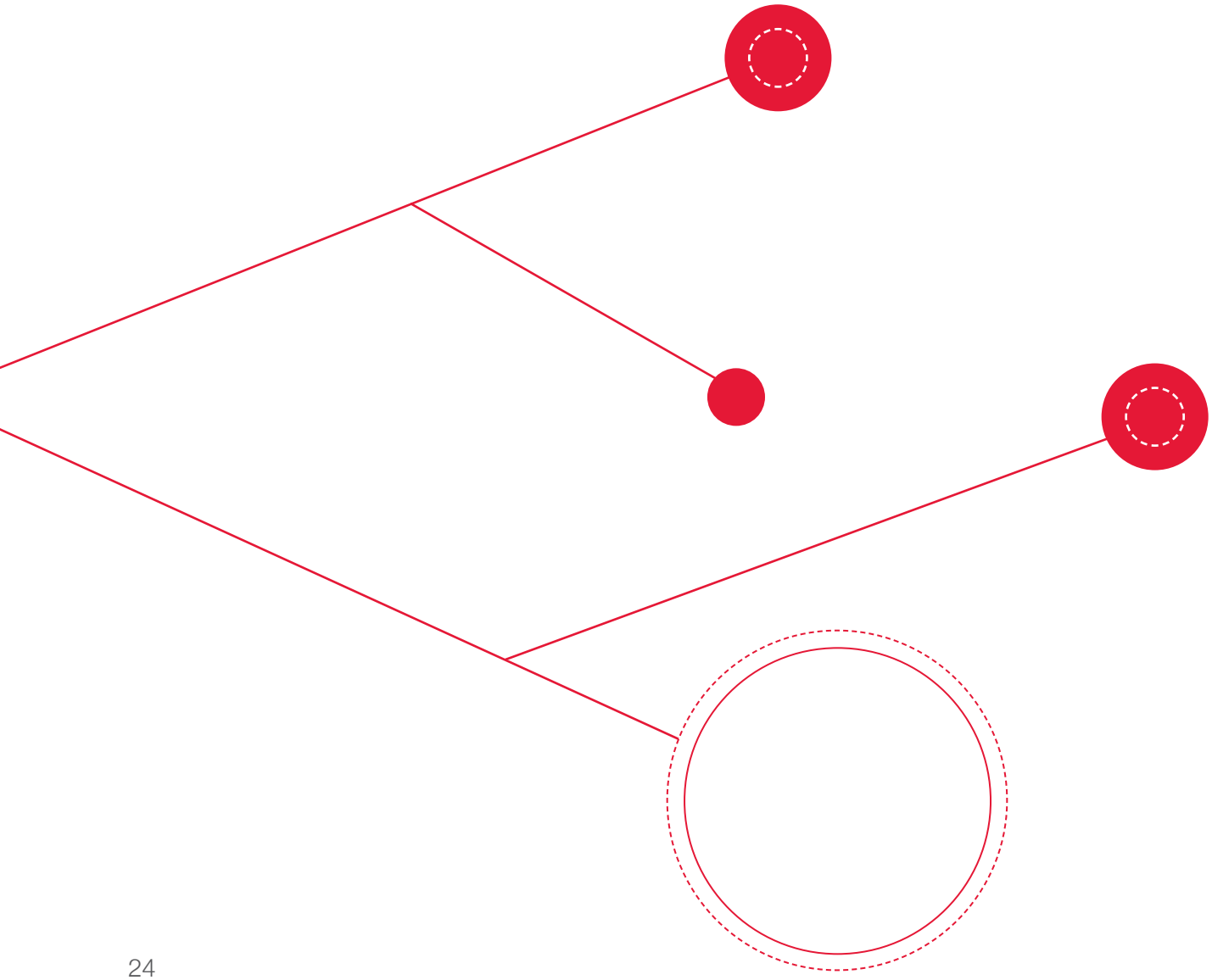
Cyber security is part of everything we do

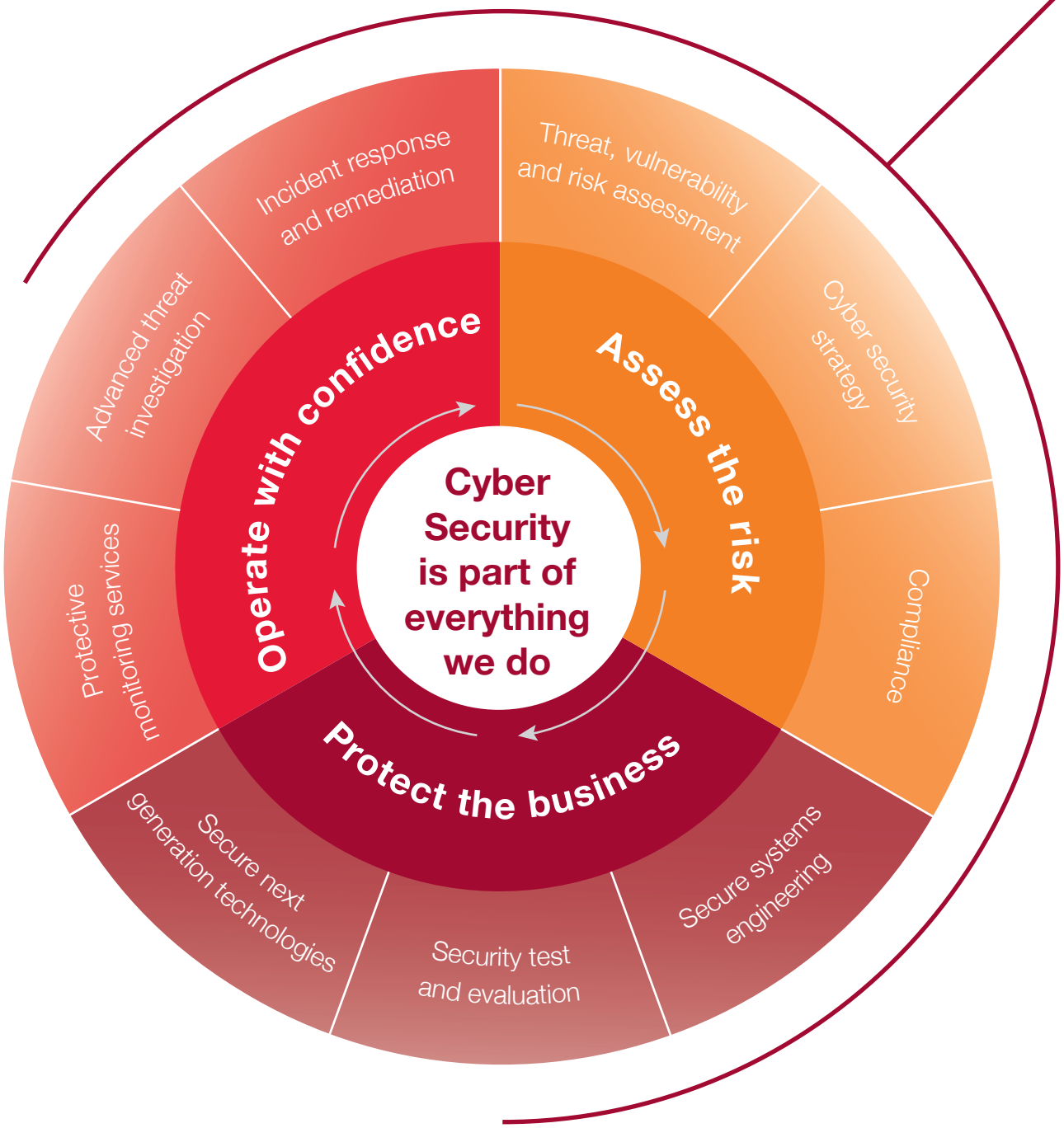
CGI applies a disciplined delivery approach that has achieved an industry-leading track record of on-time, on-budget projects. CGI has a global team of cyber security experts, who work with governments and commercial clients, ensuring their business critical systems and services are effective and secure.

CGI is one of the few providers worldwide with three accredited security certification facilities - located in the UK, Canada and the U.S. Our Security Operations Centres continuously identify and deploy the best solutions to maintain a state-of-the-art infrastructure, handling over 74 million cyber events a day.

Our high-quality business consulting, systems integration and outsourcing services help clients leverage current investments while adopting new technology and business strategies that achieve top and bottom line results. As a demonstration of our commitment, our average client satisfaction score for the past 10 years has measured consistently higher than 9 out of 10.

We help our clients grow and be more productive by offering consultancy, solutions and managed services.




Cyber Security is part of everything we do
Operate with confidence
Assess the risk
Protect the business
Incident response and remediation
Threat, vulnerability and risk assessment
Advanced threat investigation
Cyber security strategy
Protective monitoring services
Compliance
Secure next generation technologies
Security test and evaluation
Secure systems engineering

About CGI

Founded in 1976, CGI Group Inc. is the fifth largest independent information technology and business process services firm in the world. Approximately 65,000 professionals serve thousands of global clients from offices and delivery centres across the Americas, Europe and Asia Pacific, leveraging a comprehensive portfolio of services, including high-end business and IT consulting, systems integration, application development and maintenance and infrastructure management, as well as 150 IP-based services and solutions. With annual revenue in excess of C$10 billion and an order backlog exceeding C$20 billion, CGI shares are listed on the TSX (GIB.A) and the NYSE (GIB).

About Cebr

Cebr is an independent consultancy, which advises some of the world's largest companies. Cebr's reputation for insightful economic analysis, award-winning forecasting and decisive business advice is based on innovative research by a renowned team of macro and micro-economists. Since its foundation in 1993, Cebr has been 'making business sense' by applying theoretical economics backed by quantitative evidence to real world decision for FTSE firms. It provides analysis, forecasts and strategic advice to major multinationals, financial institutions, government departments, charities and trade bodies.

Cebr
Making Business Sense

CGI
Experience the Commitment®

CGI IT UK Limited, 250 Brook Drive, Green Park,
Reading RG2 6UA, United Kingdom

www.cgi-group.co.uk/cyber
enquiry.uk@cgi.com

BUILDING ON 40 YEARS OF COMMITMENT