Pierre Audoin Consultants

Premium study sponsors:

FUJITSU

Symantec

Is cyber security now too hard for enterprises?

Cyber security trends in the UK

Company profile Fujitsu Technology Solutions GmbH

About Fujitsu

Fujitsu is a Japanese IT company offering a complete range of products, services and solutions. From looking after applications and protecting data, to managing supercomputers around the world, Fujitsu helps businesses everywhere to become more innovative and efficient. Fujitsu employs 162,000 people worldwide with 14,000 people based in the UK and Ireland. For the fiscal year ending March 31, 2014, Fujitsu reported revenues of US$46 billion globally, with the UK & Ireland's annual revenue reaching £1.8 billion.

Fujitsu is committed to being a responsible business and recently achieved a 4 star rating in Business in the Community's 2014 Corporate Responsibility Index, as well as being ranked number 17 in the in Newsweek's Global Top 500 Green companies.

Over the last five decades Fujitsu has played a vital role in building and maintaining many of the services that keep the UK and Ireland working. Today, Fujitsu ICT solutions are behind many of the daily services that touch the lives of millions of people every single day. Every day, Fujitsu technology is touching lives:

- Enabling the processing of 2.8 million UK passports every year
- Helping hospitality companies serve over 570 million drinks and over 130 million meals every year
- Helping to supply energy to 12 million homes and 1 million businesses
- Providing the infrastructure for over 40% of the UK's broadband network
- Helping financial services providers to serve over 40 million customers and operate over 20,000 local branches
- Connecting 300,000 defence users in over 2,000 locations worldwide
- Helping businesses everywhere to become safer (more secure), more innovative and more efficient.

Fujitsu see's information technology as part of the bigger picture and as one of the world's largest ICT providers, it works towards bringing a prosperous future that fulfils the dreams of people throughout the world.

Company profile: Symantec

About Fujitsu

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings -- anytime, anywhere.

Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries.

Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenues of $6.7 billion.

To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

Table of Contents

Core statements I

The cyber threat landscape is getting worse, in terms of the number and type of threats and threat sources.

70% of enterprises think that the cyber security situation is worse than a year ago. Business executives feel this more acutely than IT managers, with 75% regarding the situation as worse.

Cyber security has greater focus and awareness in the boardroom.

65% of enterprises think that the focus and importance of cyber security to the board in their company has risen. No enterprises thought that it had fallen.

Cyber security workloads have increased in the last year.

More than half of firms have seen an increase in demand on their cyber security provision. The drivers for this are numerous, and include compliance concerns and the growing threat of attack.

Budgets are not increasing in line with the increased threat or rising board focus..

Less than half of respondents see their cyber security budgets growing. Cost pressures mean that enterprises cannot spend their way out of greater demands on cyber security.

Core statements II

Enterprises would prefer to increase their use of security automation.

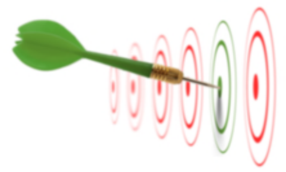
Most firms use a wide range of cyber security products and would prefer to expand the automation of security processes. But tight budgets constrain their ability to take this approach.

Firms’ preferred skills shortage response is to hire staff or retrain existing staff

To cope with the increasing workload, firms would prefer to retrain internal staff (54%) and hire in new staff (42%). Budgets and weak availability constrain their ability to do the latter.

Scarcity of skills is forcing enterprises to change behaviour.

Almost half of companies say that they outsource because they have insufficient in-house skills. Cost savings are the other major driver for outsourcing.



Enterprises reluctantly outsource security provision.

Budgets and skills shortage are driving a change in behaviour (if not attitude) towards outsourcing of cyber security.

Core statements III

Most enterprises are now considering security outsourcing (as Managed Security Services).

Driven by cost reduction and lack of internal skills
Only 26% would not consider outsourcing for any security provision

Enterprises are taking a cautious, risk-based and selective approach to Managed Security Services.

Auditing and penetration testing are the most likely areas to outsource, and some have mandated this due to independence requirements. Security management is the next most common target.

Enterprises are beginning to take interest in cyber risk insurance, though awareness remains low.

Less than a quarter of firms currently use cyber risk insurance, but 40% are considering it. Only 15% have no plans to use it.

1 Background and methodology

Introduction

Enterprises today are faced with three key challenges:

- Implementing new SMAC technologies to support the business, as part of their digital transformation programs, but while keeping it secure;
- Responding to the increasing and changing threat landscape of targeted attacks;
- Achieving and retaining compliance with an increasing number of rules and regulations.

How do enterprises respond, in the context of a nationwide shortage in cyber security skills? The skills shortage could last 20 years, according to the National Audit Office and the Select Committee on Science and Technology. PAC's own estimates suggest a shortfall of 1500 senior security architects each year. Cyber security salaries are rising at twice the industry rates.

Our hypothesis for this study was that enterprises are struggling to cope with the increase in workload, and are increasingly offloading (some of) their security provision to outsourcing providers as Managed Security Services (MSS).

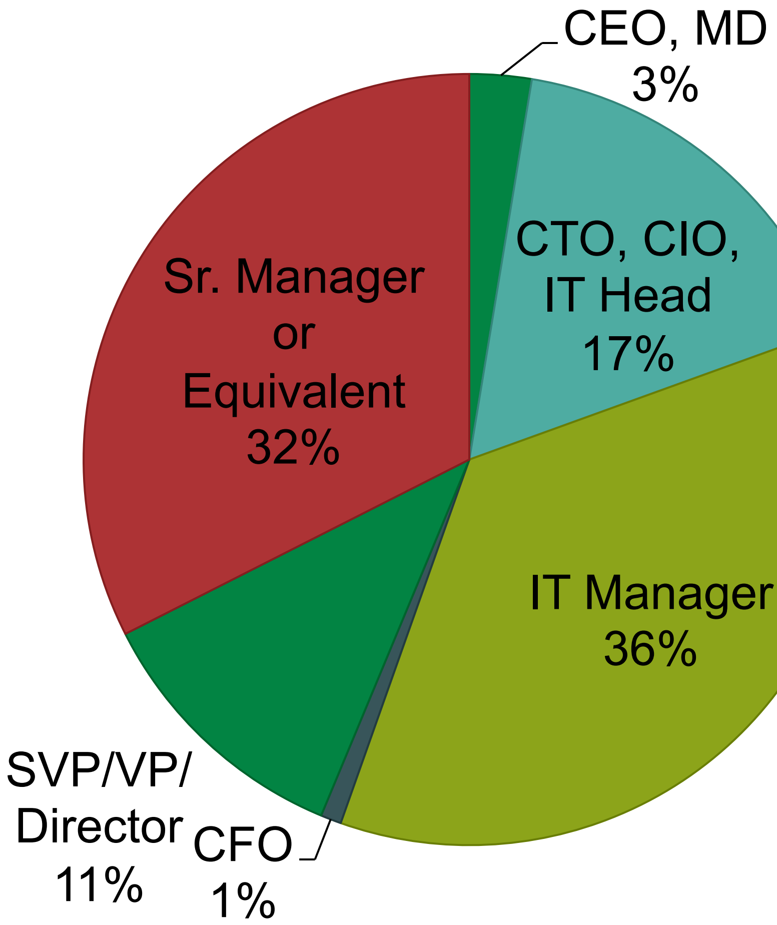
We surveyed 230 decision makers in large companies in the UK, to understand their motivations and drivers with regard to cyber security provision.

This study deals with the following **questions**:

- What do companies understand about the growing cyber threat landscape?
- How are companies meeting their resource challenges in cyber security?
- How are they using external providers to meet resource challenges?
- What are the drivers and inhibitors for using external cyber security providers?
- What alternative approaches to external cyber security provision being considered?
- Which services do companies expect from a cyber security provider?
- What are the capabilities and attributes of a credible cyber security provider?

230 respondents from UK enterprises

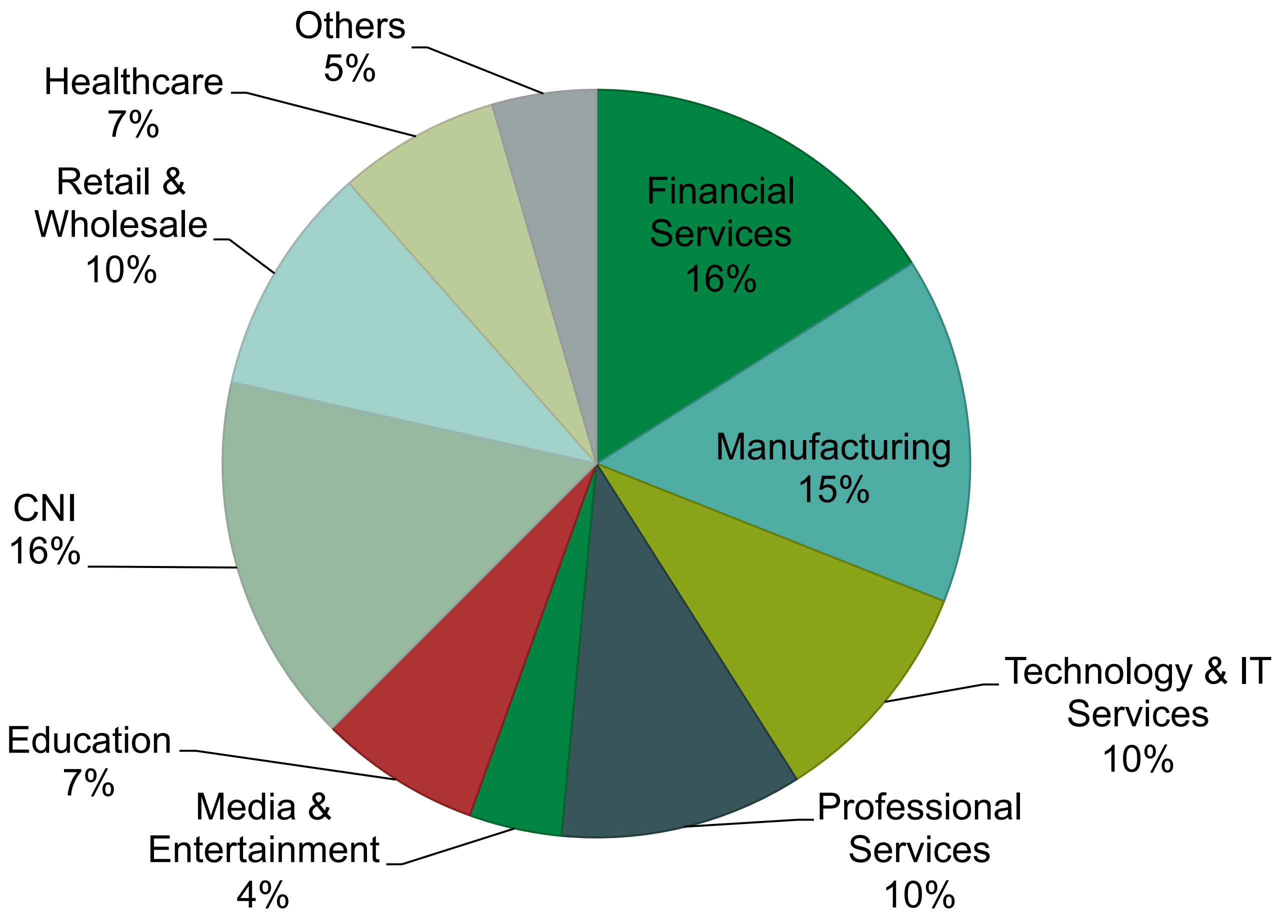
ITDM = 122 (53%)
BDM = 109 (47%)



Between October and November **2014, 230 executives at UK companies with over 1000 employees** were surveyed by telephone (CATI).

n=230

UK companies with 1000+ employees in commercial sectors

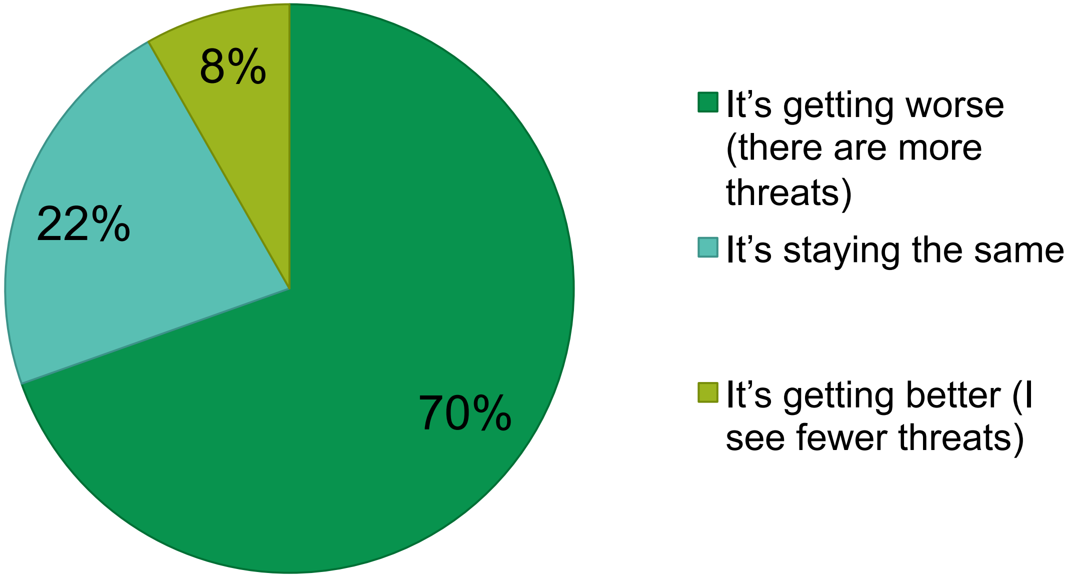


CNI = critical national infrastructure firms (transport, energy & Utilities, and telecoms)

n=230

2 Enterprises’ outlook on cyber security

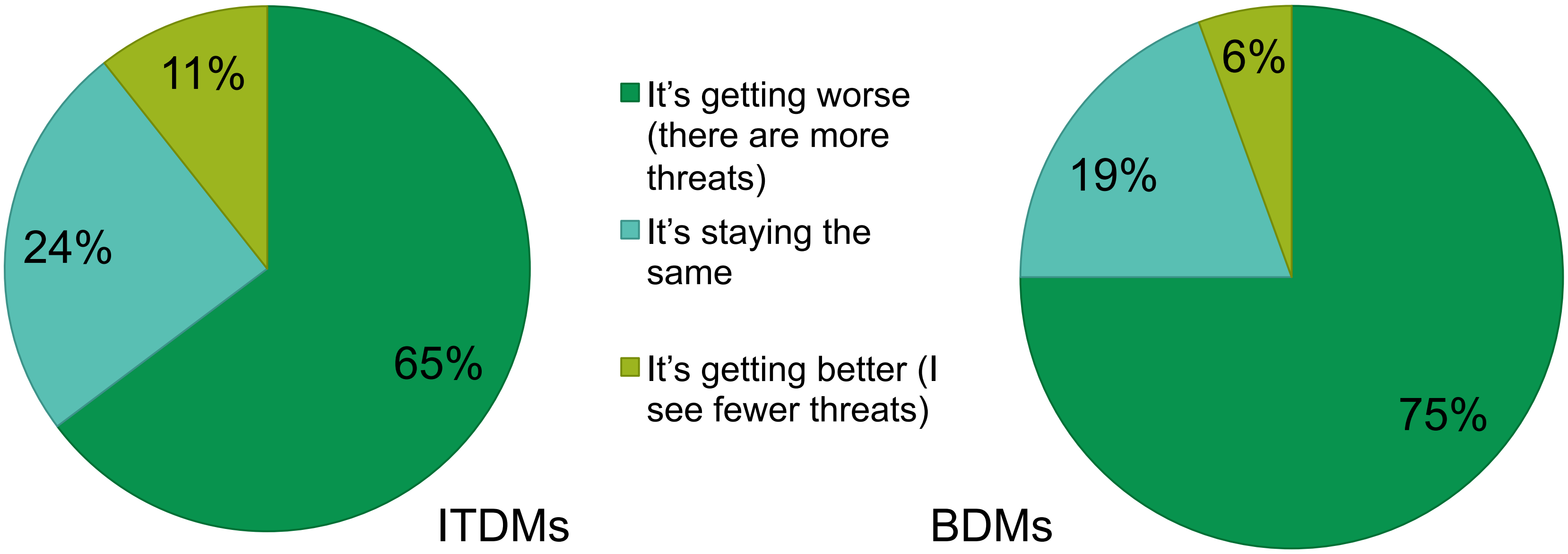
What is your view of the cyber threat landscape, in terms of the number and type of threats and threat sources you see or are aware of?



An overwhelming majority of enterprises see the cyber threat getting worse. This is not a surprise, but it does enable us to quantify the scale and extent of enterprises' perception regarding the cyber landscape. As our figure shows, 70% of respondents believe that the situation is getting worse. We believe that this is caused in part by respondents' own experience within their firms and partly by the greater exposure to cyber security breaches in the national and trade press.

n=230

What is your view of the cyber threat landscape, in terms of the number and type of threats and threat sources you see or are aware of?



Interestingly, the business audience has a more negative view of the cyber security situation than IT professionals. This indicates that cyber security breaches are gaining more notoriety at a business level, as exemplified by greater coverage in the national and business press. We think there is also a tendency for IT professionals to claim that they are on top of the situation, and thereby reporting that the situation is not altogether weaker. Nevertheless, still two-thirds of IT executives see the situation as getting worse.

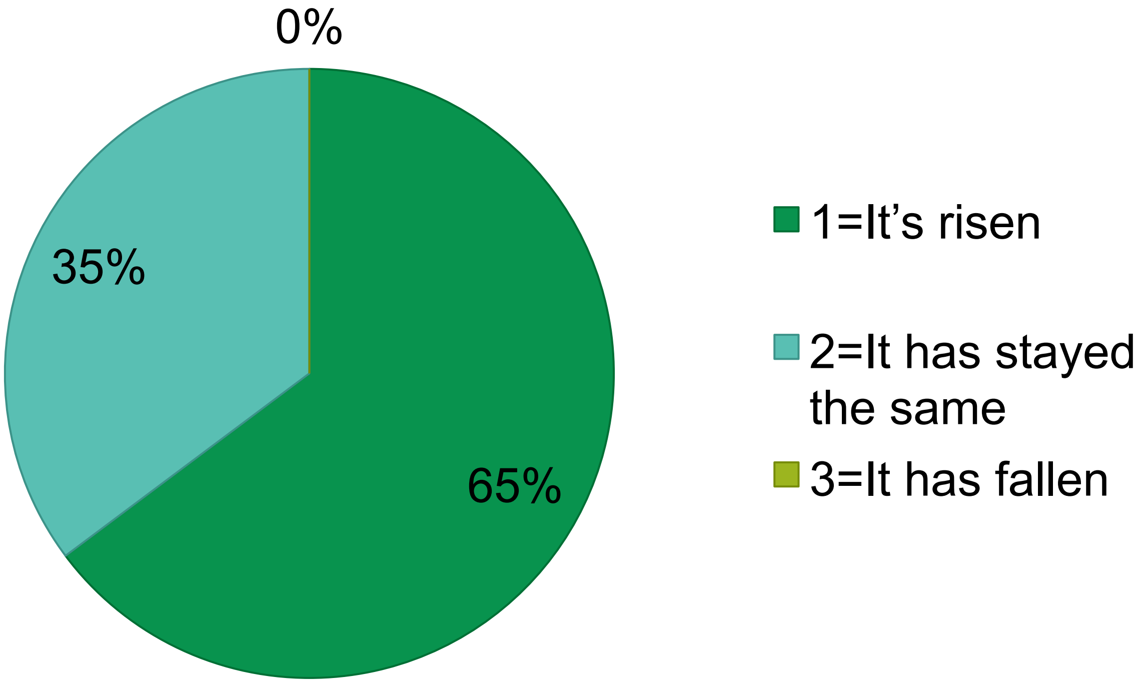
n=230

Industry View

CNI (84%) & Financial Services (78%) are more likely than average (70%) to regard the threat landscape as getting worse

Professional Services is less likely (52%) than average (70%) to see an increased workload

Has the focus and importance of cyber security to the board in your company risen or fallen in the last year?



Two-thirds of our respondents see the focus and importance of cyber security at board level rising in the past year. This is strong evidence to suggest that cyber security is regarded as a primary risk to business operations, and one would expect a commensurate rise in resource provision. However, as we shall see, this is not the case.

n=230

How do you gain your board’s interest in cyber security?

“Security is one of the important things in our company. I think that's our **highest priority**, always.”

“Emphasizing **threats** related to personal devices and IT equipment used by directors to make threats more **understandable**.”

“By advising them of risks/ **consequences** of doing nothing”

“We have **business continuity** meeting where we explain them what is happening, give **different options**, and ask what they feel about it.”

“By detailing the amount of **loss** we could incur (both direct financial and in-direct financial loss, via the potential **loss of customer confidence** with us as a company).”

“We have a **formal risk program** and we regularly report security instances **at all levels** and make them aware of global and newsworthy events.”

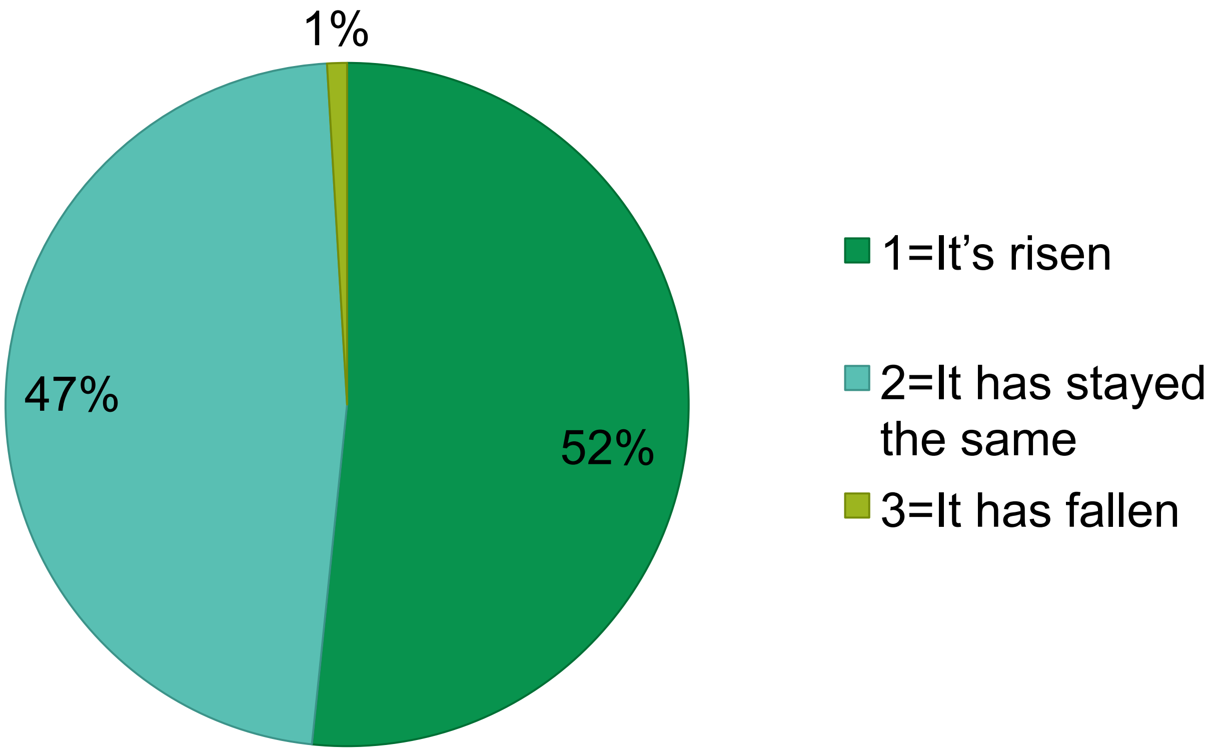
“It's **a rolling item** on our agendas, board meetings; we always have IT & security on those meetings.”

“Have to show how it would **affect** the company.”

“Its mainly through **risk analysis**.”

“Understanding the risk of possible **financial and reputational loss**, a clear understanding of impact and giving them **remediation options**.”

Has the cyber security workload increased for your department in the last year?

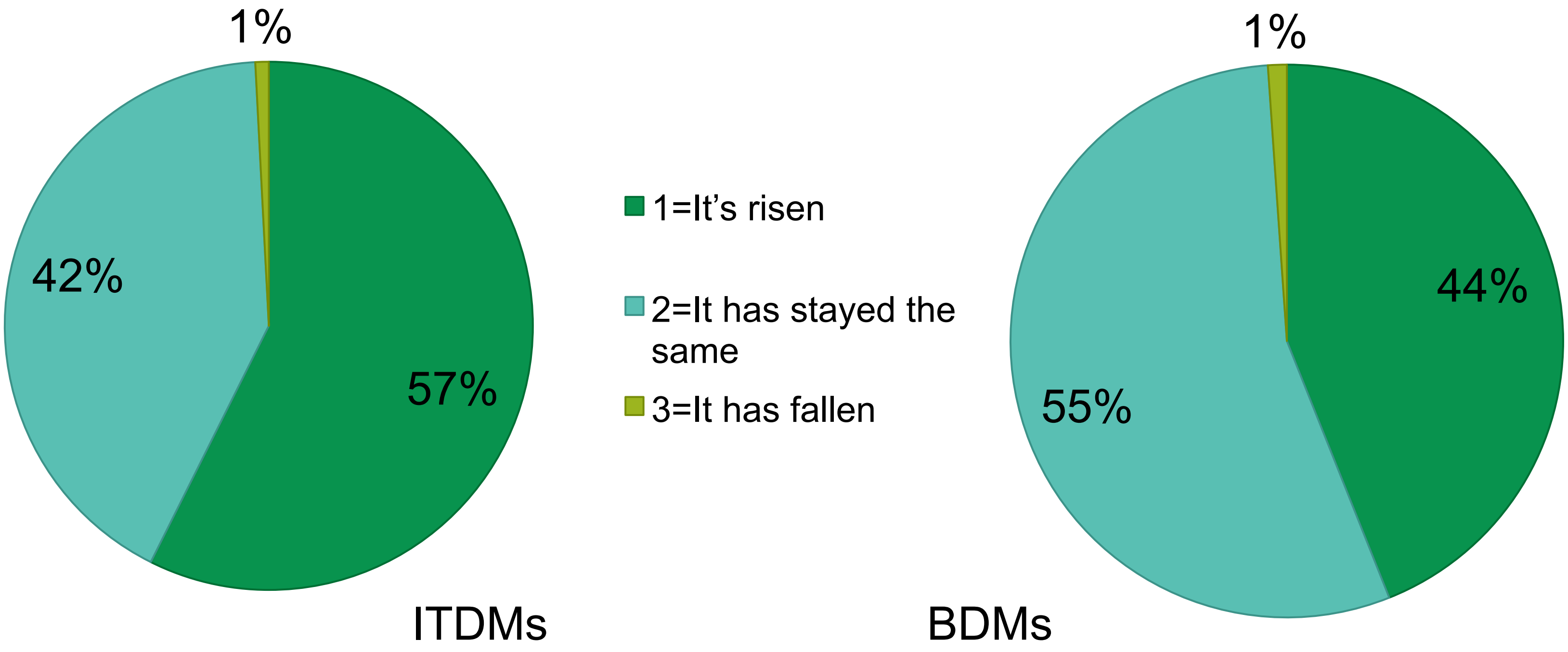


Over half of our sample sees the workload for the cyber security department increasing in the past year. This is to be expected, given the worsening cyber landscape situation and increased board attention. It is interesting, though, that just under half of our respondents have not seen an increase in workload, suggesting that, for some companies, they are coping with the situation using existing resources.

There is a strong correlation between those companies seeing a workload increase and a propensity to outsource.

n=230

Has the cyber security workload increased for your department in the last year?



We see from this chart that the increase in workload is experienced largely by the IT department, which feels the pain much more acutely than business executives. Again, this is to be expected, given that most cyber security provision is supplied by IT. Perhaps IT needs to explain the consequences of the worsening situation to business more effectively, in order to convey and increase in workload and availability of budget and resources.

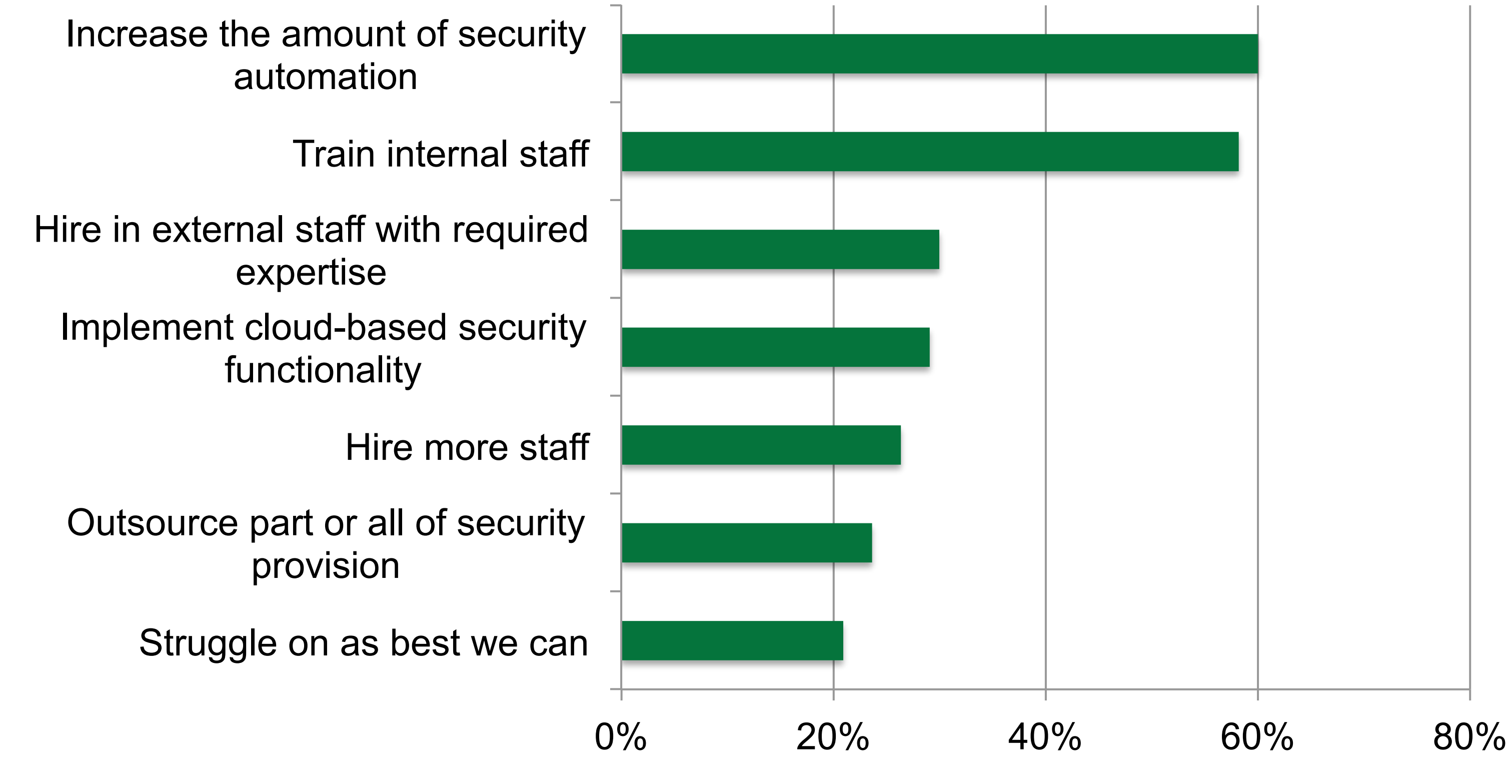
n=230

Industry View

Manufacturing is more likely (66%) than average (52%) to see an increased workload

Education is less likely (40%) than average (52%) to see an increased workload

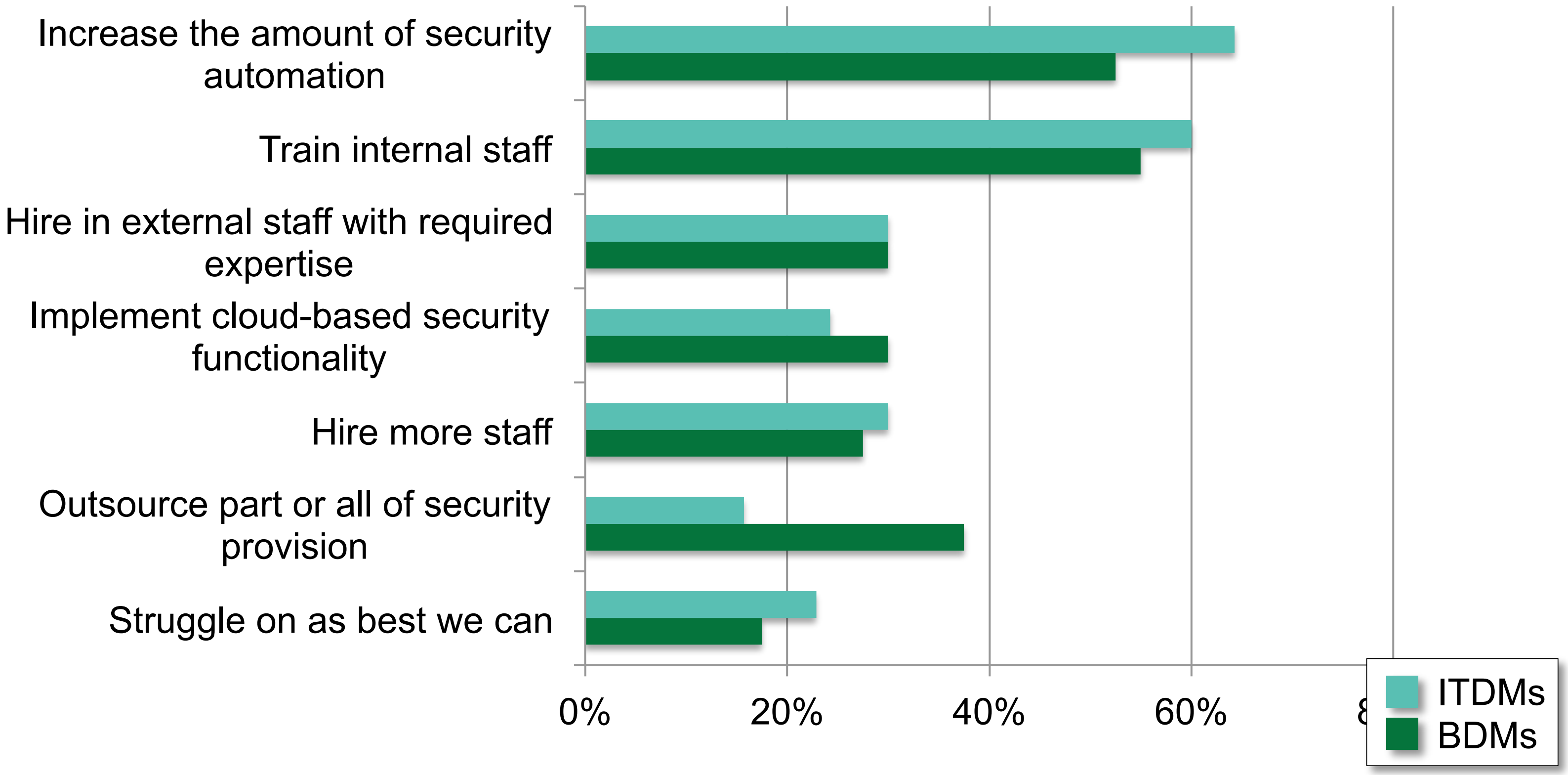
What is your current approach to the increased workload? (Select up to three)



Of those firms citing an increased workload in cyber security, their preferred approach in response is to increase the amount of security automation, closely followed by training internal staff. There is a clear reluctance to outsource part or all of security provision, and this is a common theme throughout our survey. Interestingly, 21% of respondents agreed that they is struggling on as best they can, suggesting a severely restricted budgeting and resourcing climate.

n=110

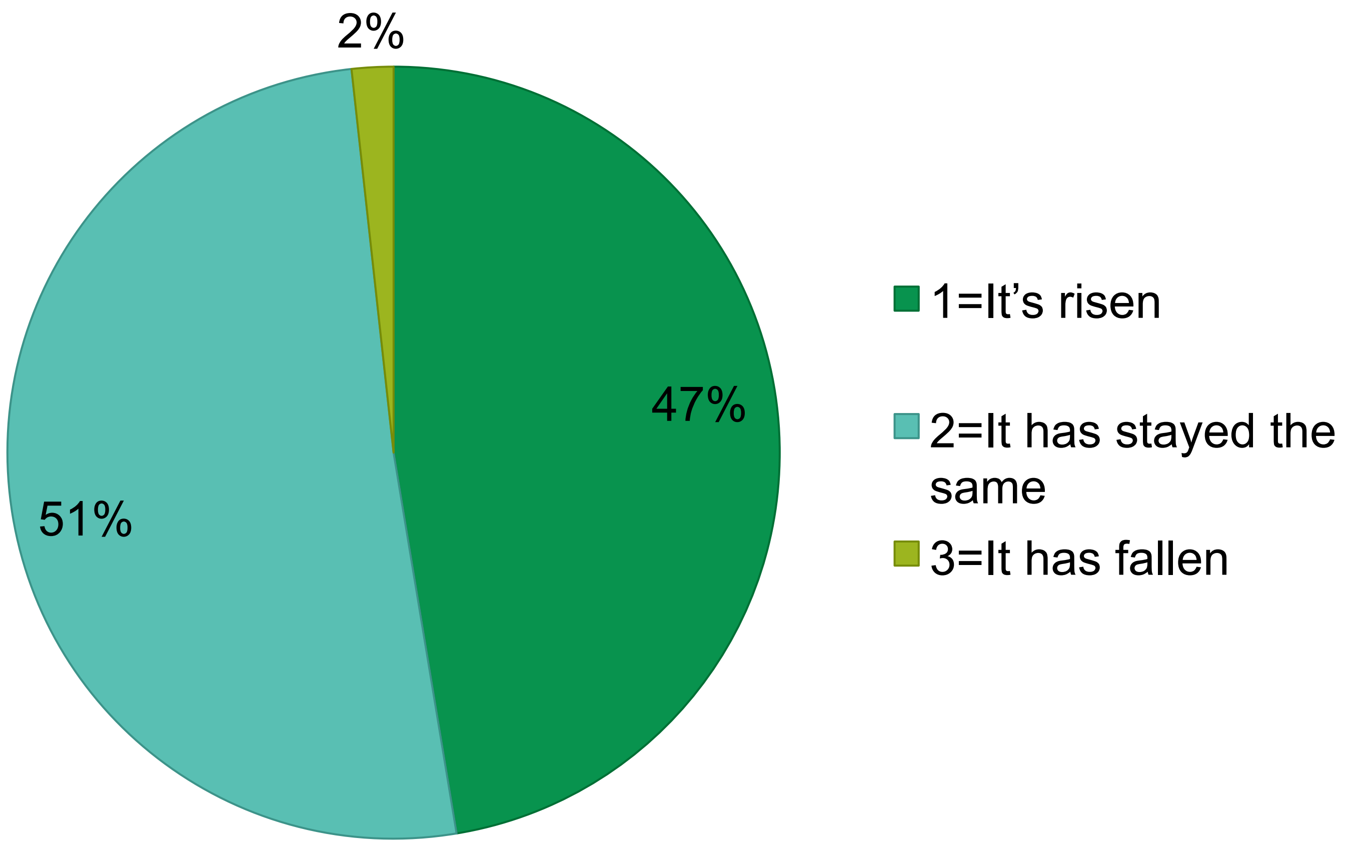
What is your current approach to the increased workload? (Select up to three)



The main difference between IT executives and business managers is shown in the response to being asked about outsourcing. We can see from the chart above that business people are much more willing to outsource security provision than IT people, presumably because IT is typically responsible for security delivery (and therefore has more concerns over operational control, job security, and so on).

n=110

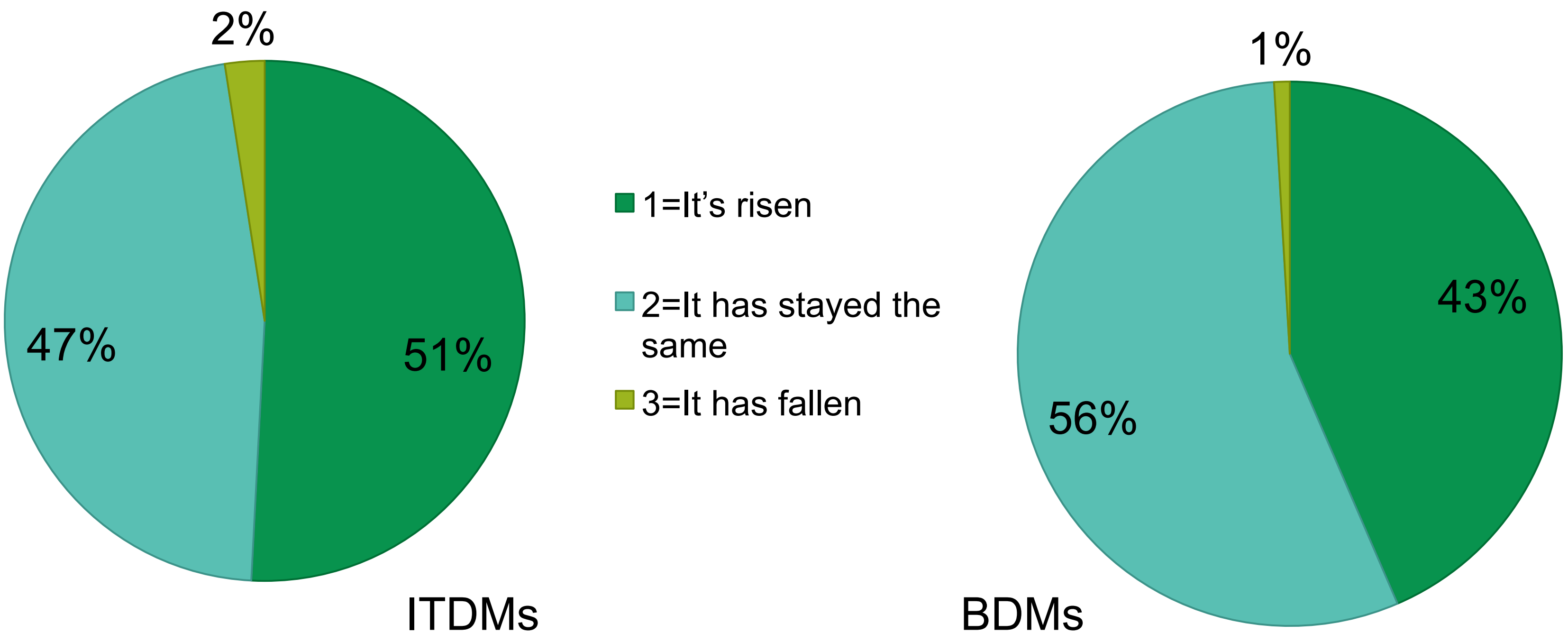
Has the cyber security budget risen or fallen



Less than half of organisations surveyed are seeing their cyber security budgets rise. This could be seen as a good thing, given that a full 47% of firms on investing in cyber security. But if this chart is compared with the earlier picture showing a worsening cyber security situation, it demonstrates a funding gap. In other words, there are more organisations seeing a worsening situation than there are committed to increasing cyber security budgets.

n=230

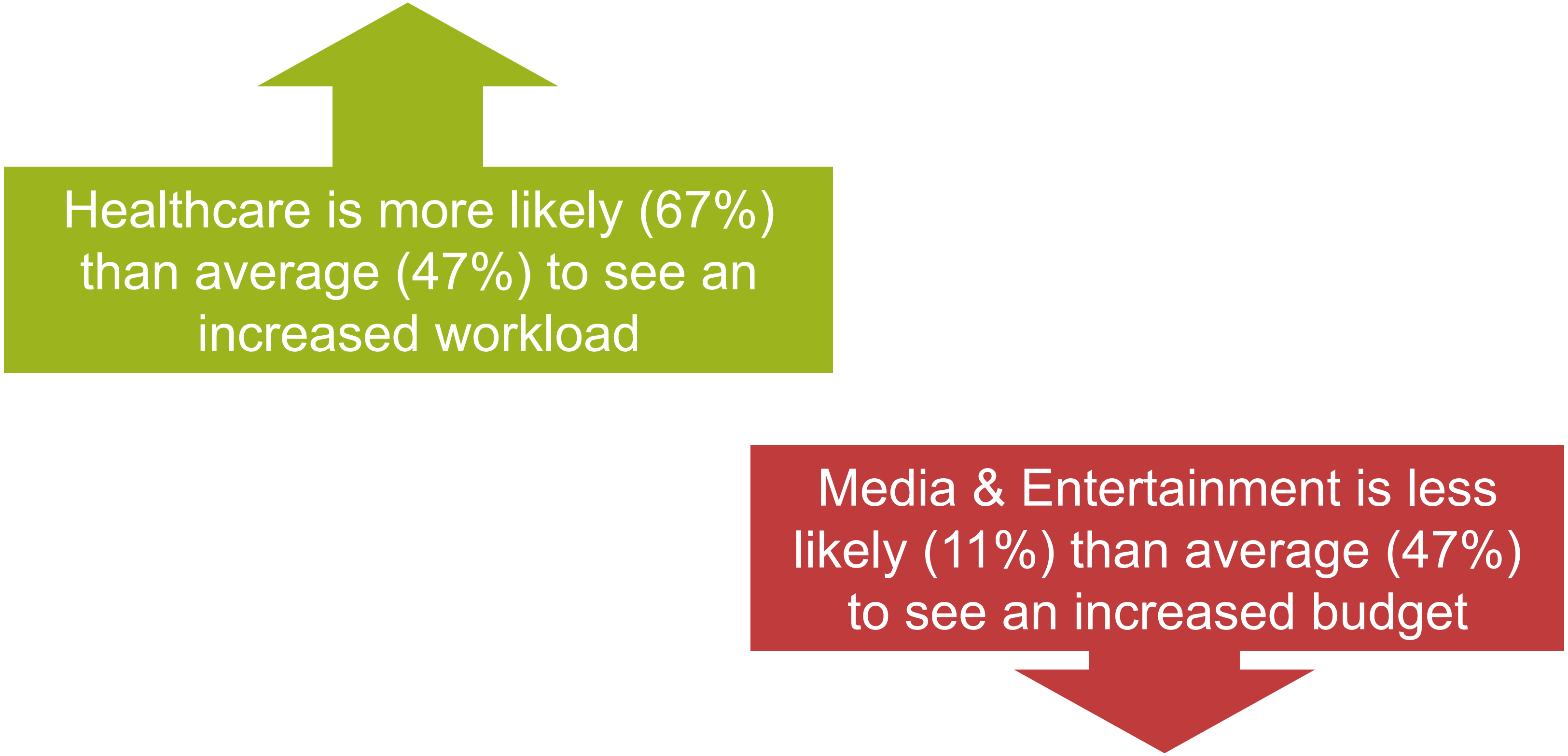
Has the cyber security budget risen or fallen in the last year?



Comparing IT and business views of budget increases, we can see that a slim majority of IT people see their cyber security investment rising. But far fewer business executives have the same degree of optimism.

n=230

Industry View



Healthcare is more likely (67%) than average (47%) to see an increased workload

Media & Entertainment is less likely (11%) than average (47%) to see an increased budget

Interim conclusion

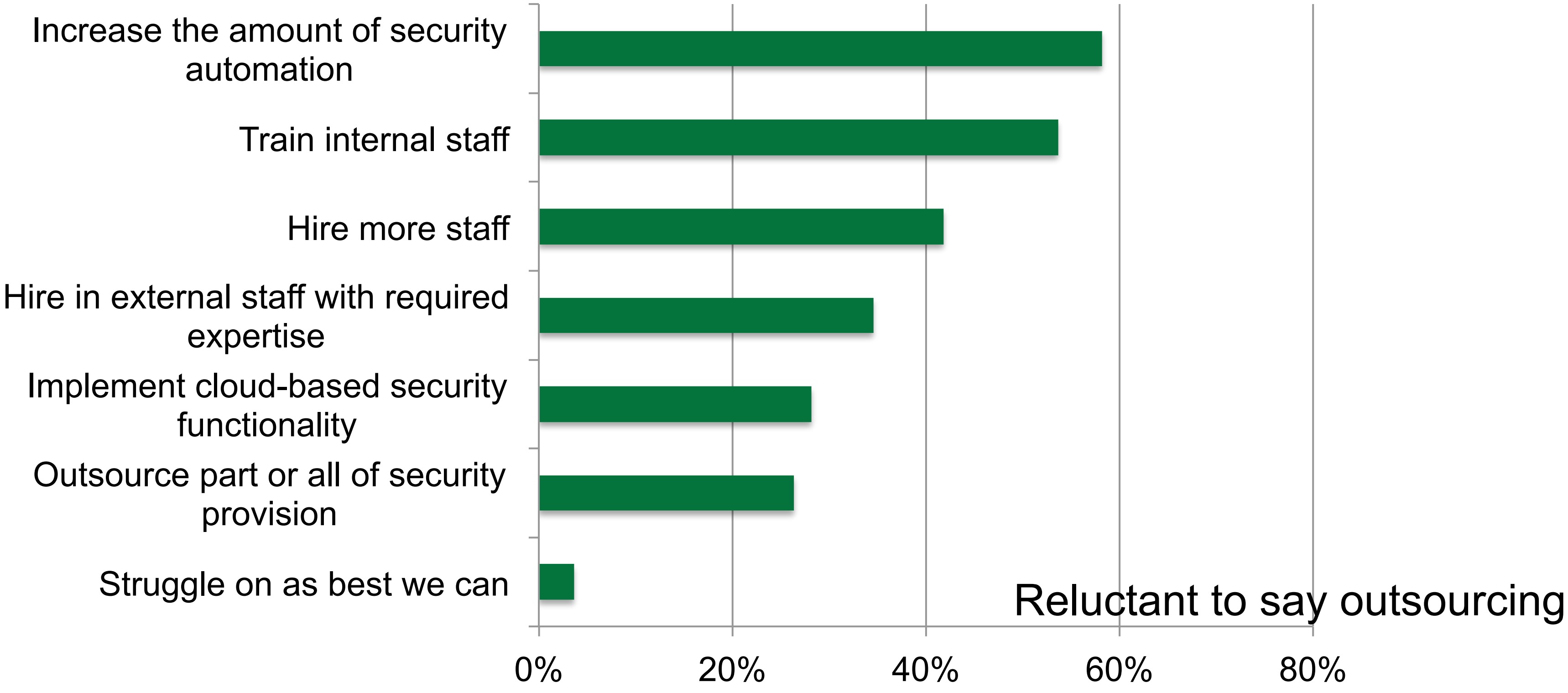
The overall picture of cyber security provision in large organisations is that the threat landscape is getting worse, board attention and focus is increasing, but there is a funding shortfall in many organisations.

Firms' preferred approach to this is to increase the amount of security automation, followed by training of internal staff. There is a clear reluctance (or inability) to hire external staff and a tangible antipathy towards outsourcing.

However, as we will explore in the next section, organisational reluctance to outsourcing does not necessarily translate into practice, with more organisations admitting to using external resources than would prefer to do so (all other things being equal).

3 Enterprises’ cyber security strategy

And what would you like to do in your approach to the increased workload? (Select up to three)

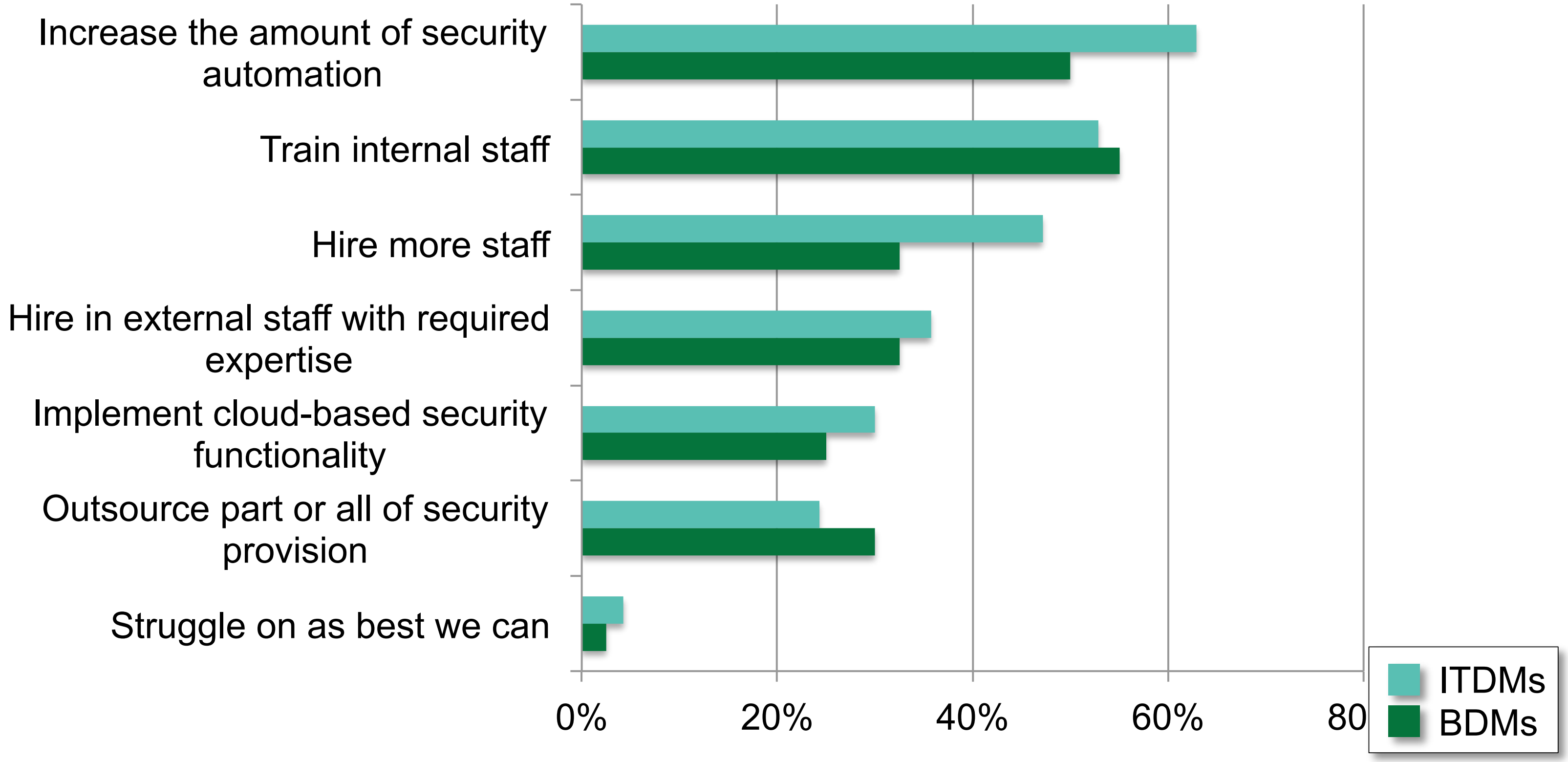


Reluctant to say outsourcing

We also asked to companies to cite their preferred approach (as opposed to their current method of working). In contrast to current practice, more organisations would like to hire more staff or even bring in external staff with appropriate expertise. Still, organisations appear reluctant to revert to outsourcing to solve their security provision issues. Encouragingly, very few organisations are happy to struggle on as best they can.

n=110

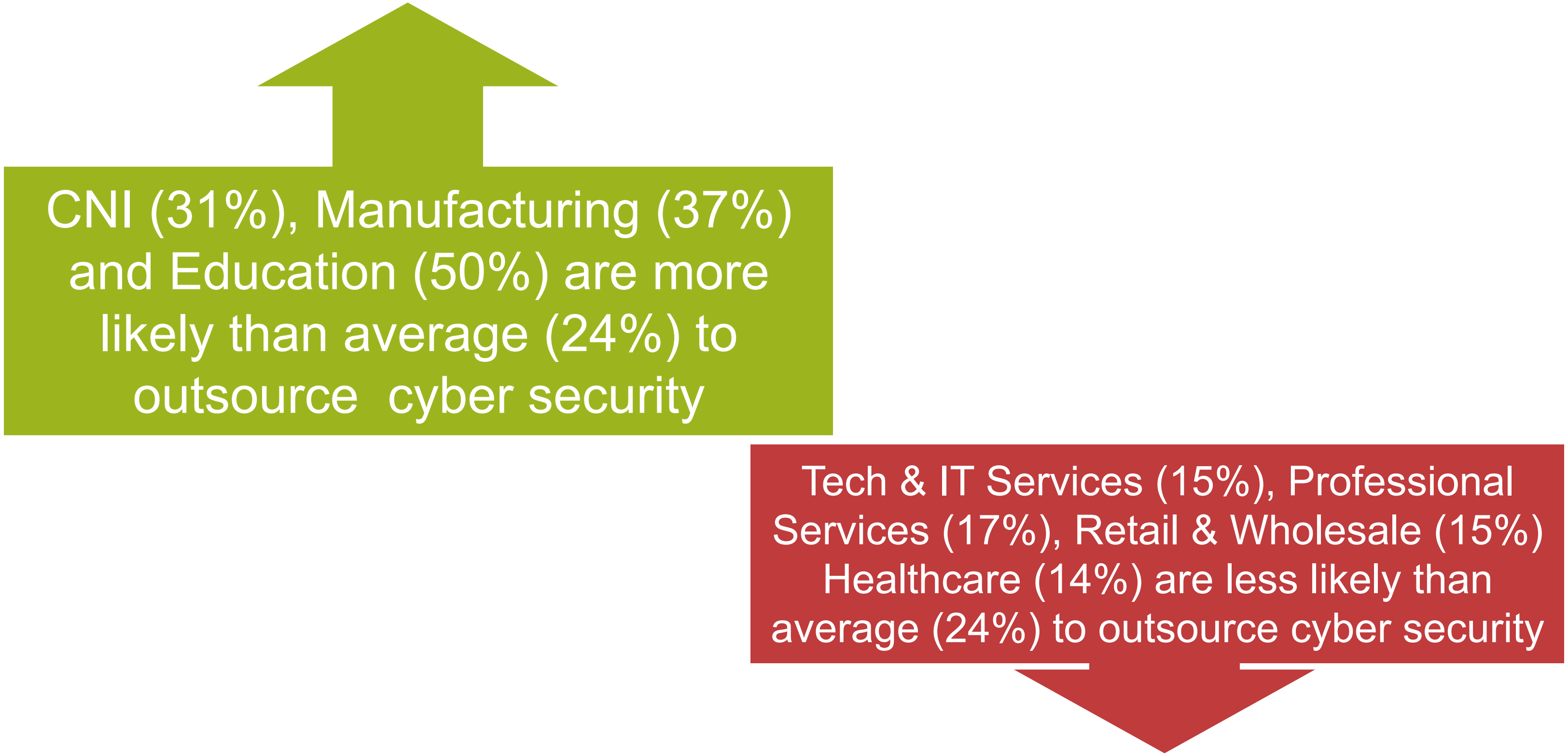
And what would you like to do in your approach to the increased workload? (Select up to three)



Here we see core differences between IT and business preferences, with IT managers preferring a more technical solution through automated security. Business executives are more willing to adopt outsourcing as a means of alleviating the increased workload. Interestingly, business people are much less willing to adopt cloud-based security functionality.

n=110

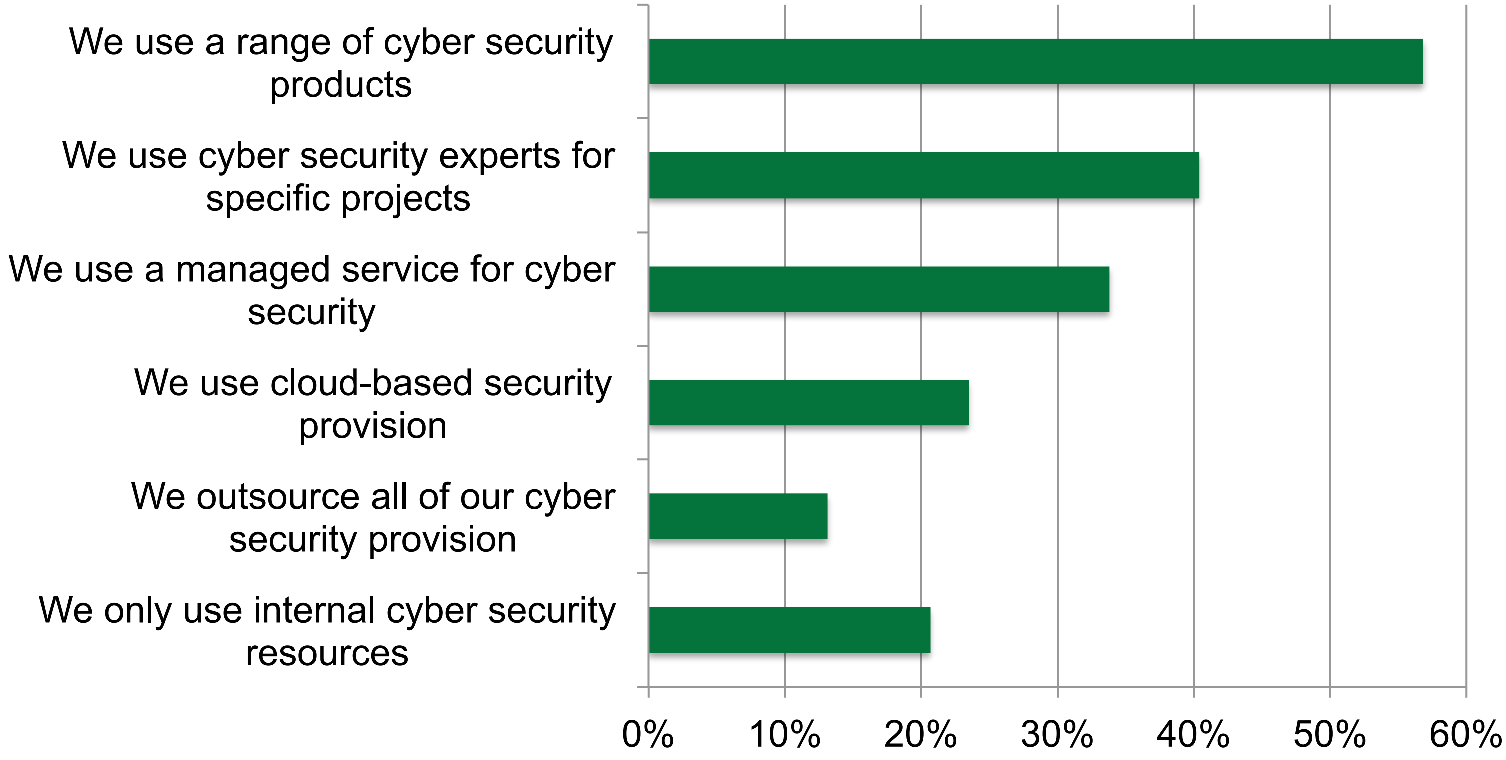
Industry View



CNI (31%), Manufacturing (37%) and Education (50%) are more likely than average (24%) to outsource cyber security

Tech & IT Services (15%), Professional Services (17%), Retail & Wholesale (15%) Healthcare (14%) are less likely than average (24%) to outsource cyber security

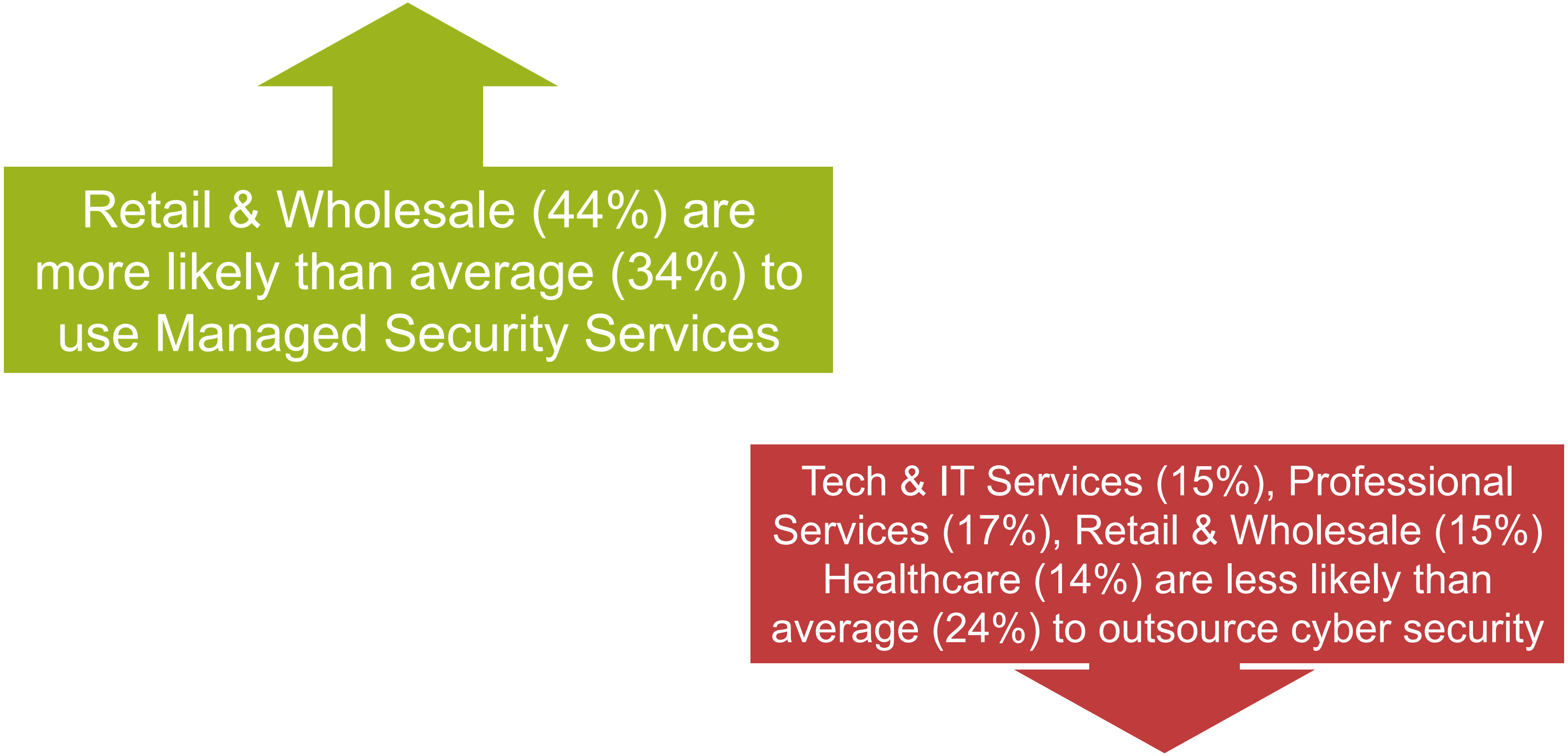
To what extent are you using external providers to meet cyber security resource challenges? (Select all that apply)



This chart reveals the true extent of the use of external provision for cyber security in large UK companies. It shows that the most common type of external support is the use of security products. However, 40% of companies buy in security expertise for specific projects, 34% use Managed Security Services (that is, outsourcing), and 13% outsource all cyber security provision. Only 21% of firms use no external cyber security resources.

n=230

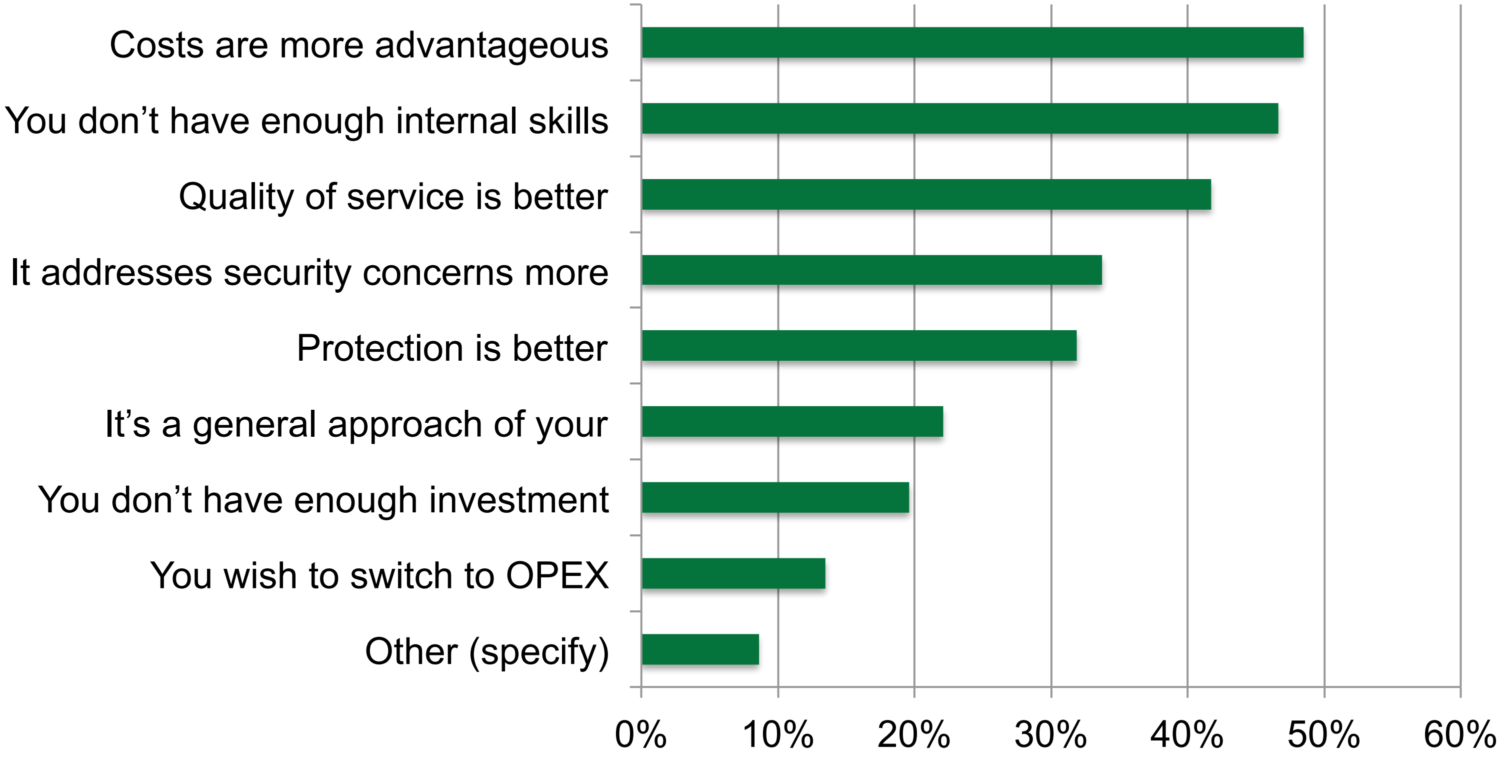
Industry View



Retail & Wholesale (44%) are more likely than average (34%) to use Managed Security Services

Tech & IT Services (15%), Professional Services (17%), Retail & Wholesale (15%) Healthcare (14%) are less likely than average (24%) to outsource cyber security

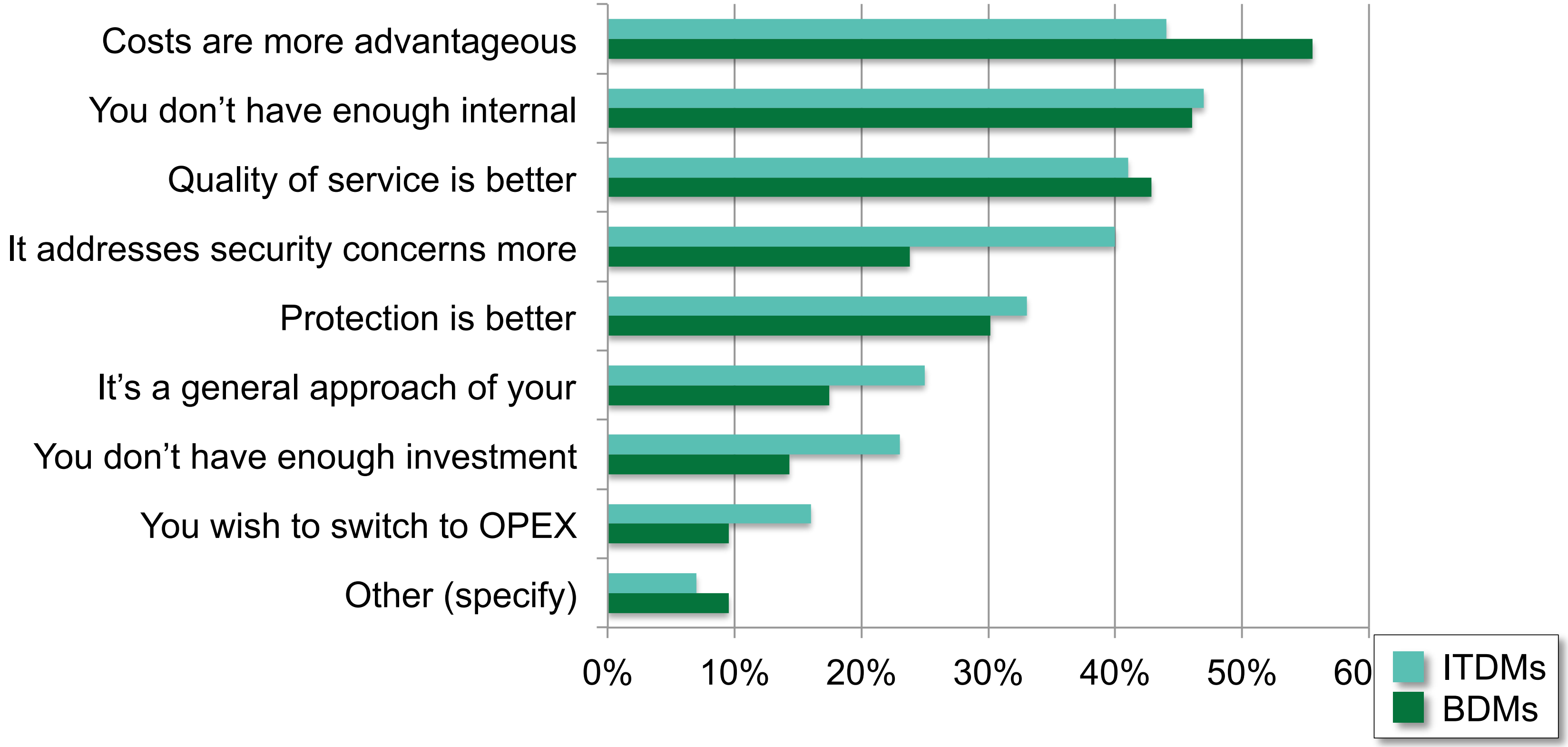
Why did you decide to outsource ? Several possible answers



The reasons for using external resources are varied, but the most common cited are costs and lack of internal skills. Service improvements, including quality of service, speed of provision and better protection are also important, possibly as side benefits to the main drivers of cost and skills.

n=163

Why did you decide to outsource ? Several possible answers



There are some important differences between IT and business use on the reasons to outsource. Costs appear more important to business executives, whereas speedier provision of capability is considerably more important to IT people.

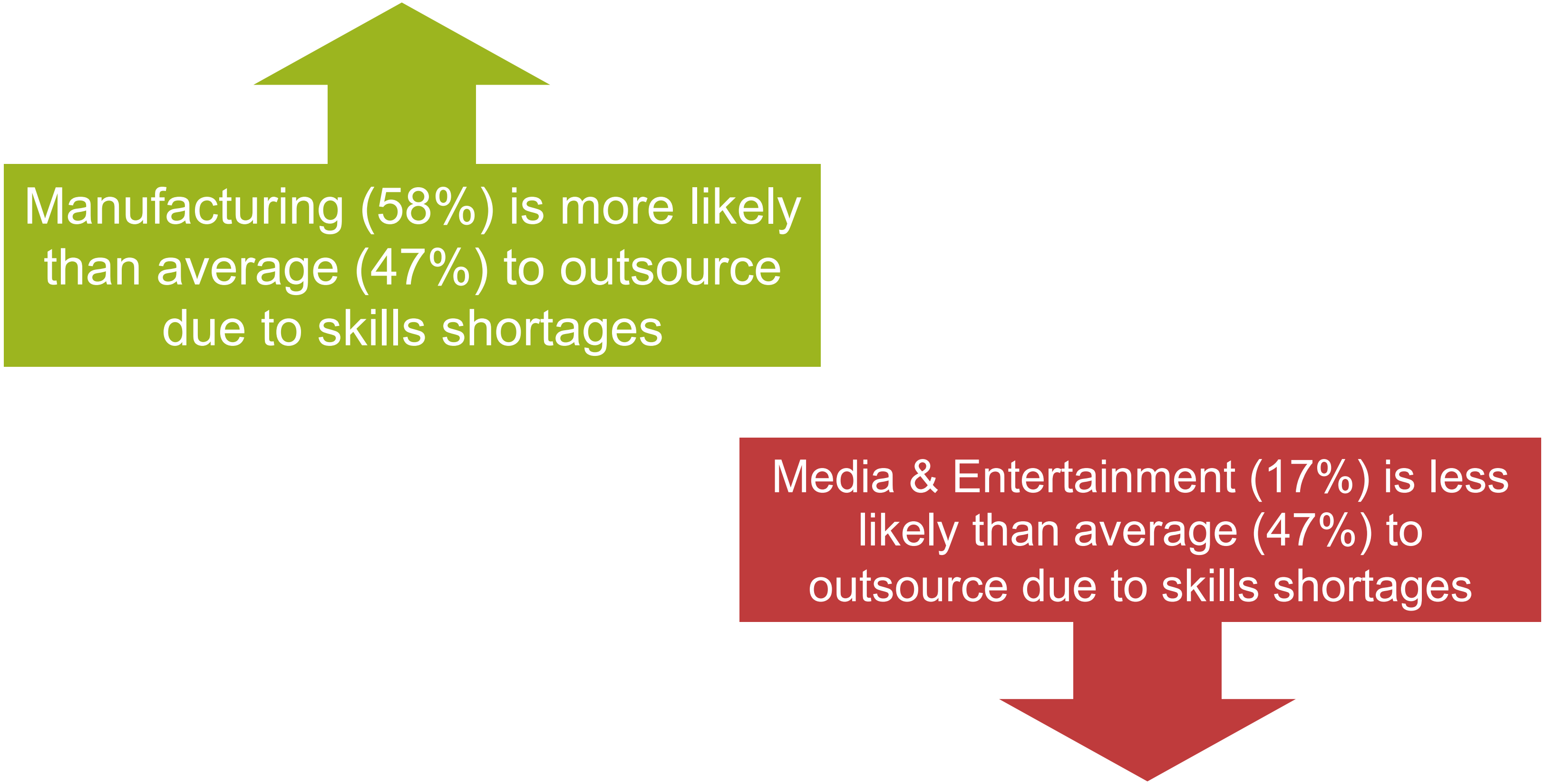
n=163

Industry View

Professional Services (67%) and Media & Entertainment (83%) are more likely than average (48%) to outsource for cost reasons

Tech & IT Services (33%) and Retail & Wholesale (35%) are less likely than average (48%) to outsource for cost reasons

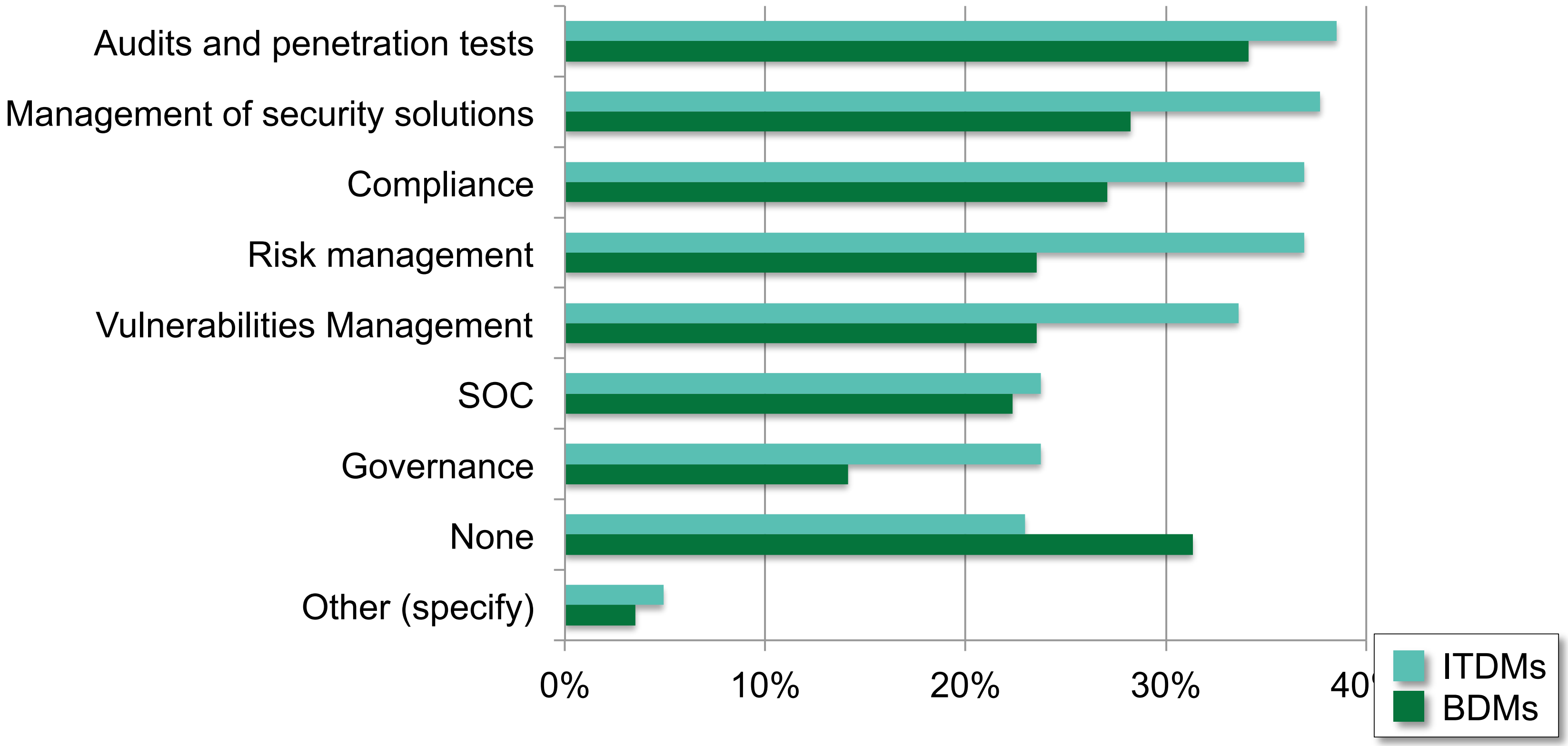
Industry View



Manufacturing (58%) is more likely than average (47%) to outsource due to skills shortages

Media & Entertainment (17%) is less likely than average (47%) to outsource due to skills shortages

What other parts of your IT security could you outsource in the future?



Asked about possible future outsourcing plans, we determined a broad range of areas as potential targets for outsourcing. None of these attracted a majority of respondents. However it is no surprise to see that audits and penetration testing tops of the chart, as these are activities traditionally conducted by external (or a least independent) providers.

Importantly, only 26% of firms say they would not outsource cyber security in any case.

n=207

Interim conclusion

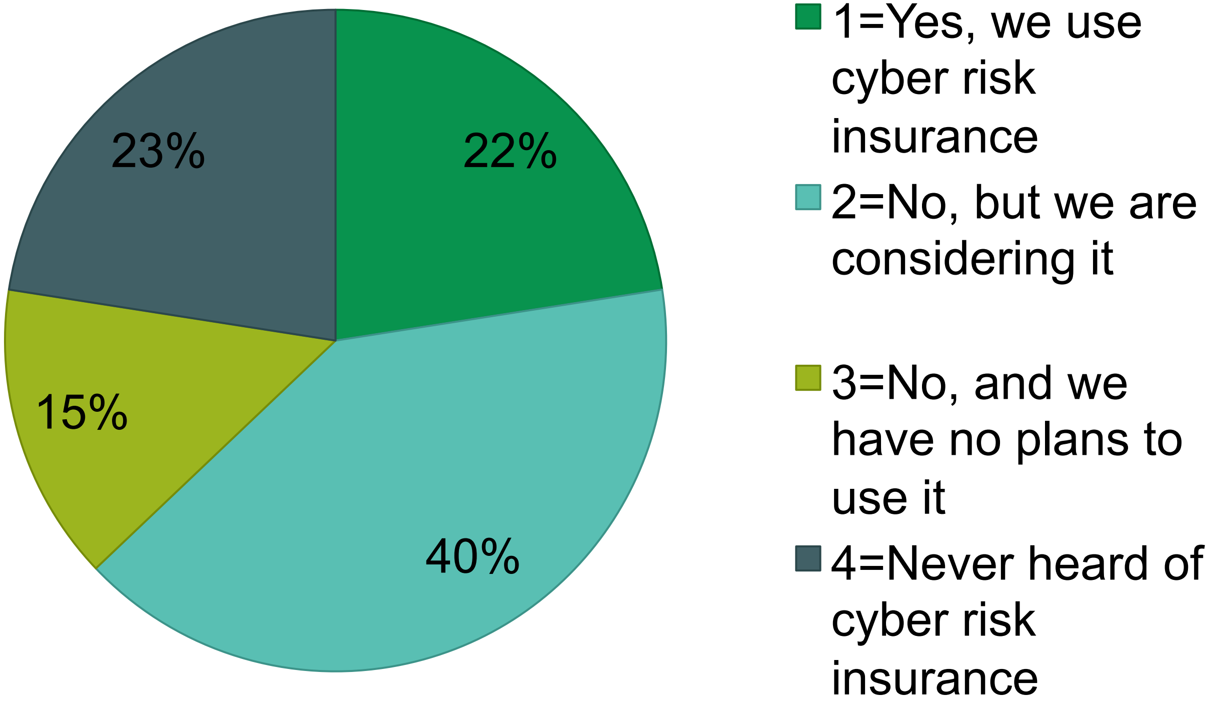
Our research shows that organisations have an innate reluctance to outsource, and this even extends to admitting that outsourcing goes on. But by drilling down into actual practice we discover that there is a high degree of use of external provision, including outsourcing. The prevalent method of using external provision is by buying in expertise on a project-by-project basis.

The overall motivation for using external provision, including outsourcing, is a combination of a lack of funds and expertise, echoing our earlier findings which identified a funding gap. The double whammy of insufficient funds and a scarcity of skills appears to be driving organisations towards external resources, including outsourcing, even though there is a clear reluctance to do this.

This represents an entirely pragmatic approach, according to PAC. Organisations dislike losing visibility and control of processes, especially those that have a high risk profile such as cyber security. But the pressures on budgets and expertise are such that companies have little option but to use external providers.

4 Awareness and adoption of Cyber Risk Insurance

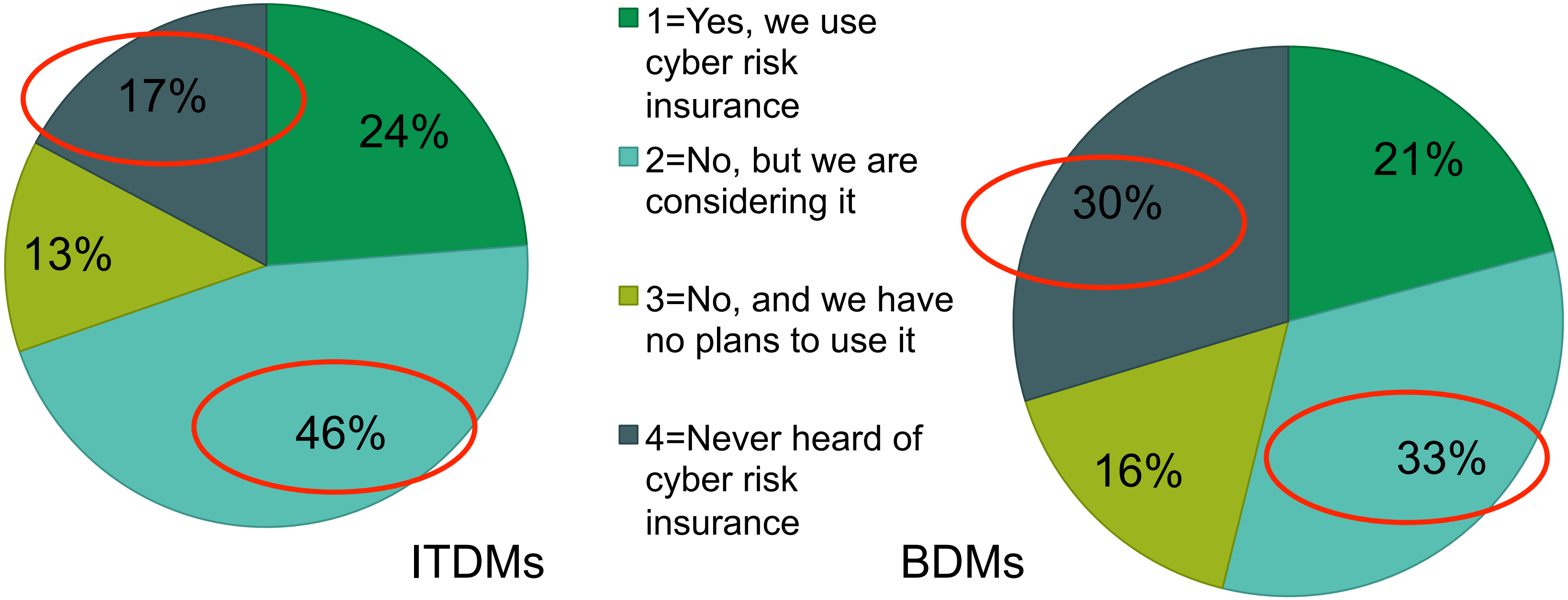
Are you using cyber risk insurance (also known as cyber liability insurance or cyber breach insurance)?



Cyber risk insurance is a relatively new concept in the UK, although it is widely used in the US. It has increased in awareness over the last 18 months, so we were interested to examine the extent of the awareness, and adoption plans. We were surprised to see that almost one quarter of our sample is already using cyber risk insurance. A further 40% are considering it. 38% of respondents have either no plans to use this type of insurance or in fact have never heard of it.

n=230

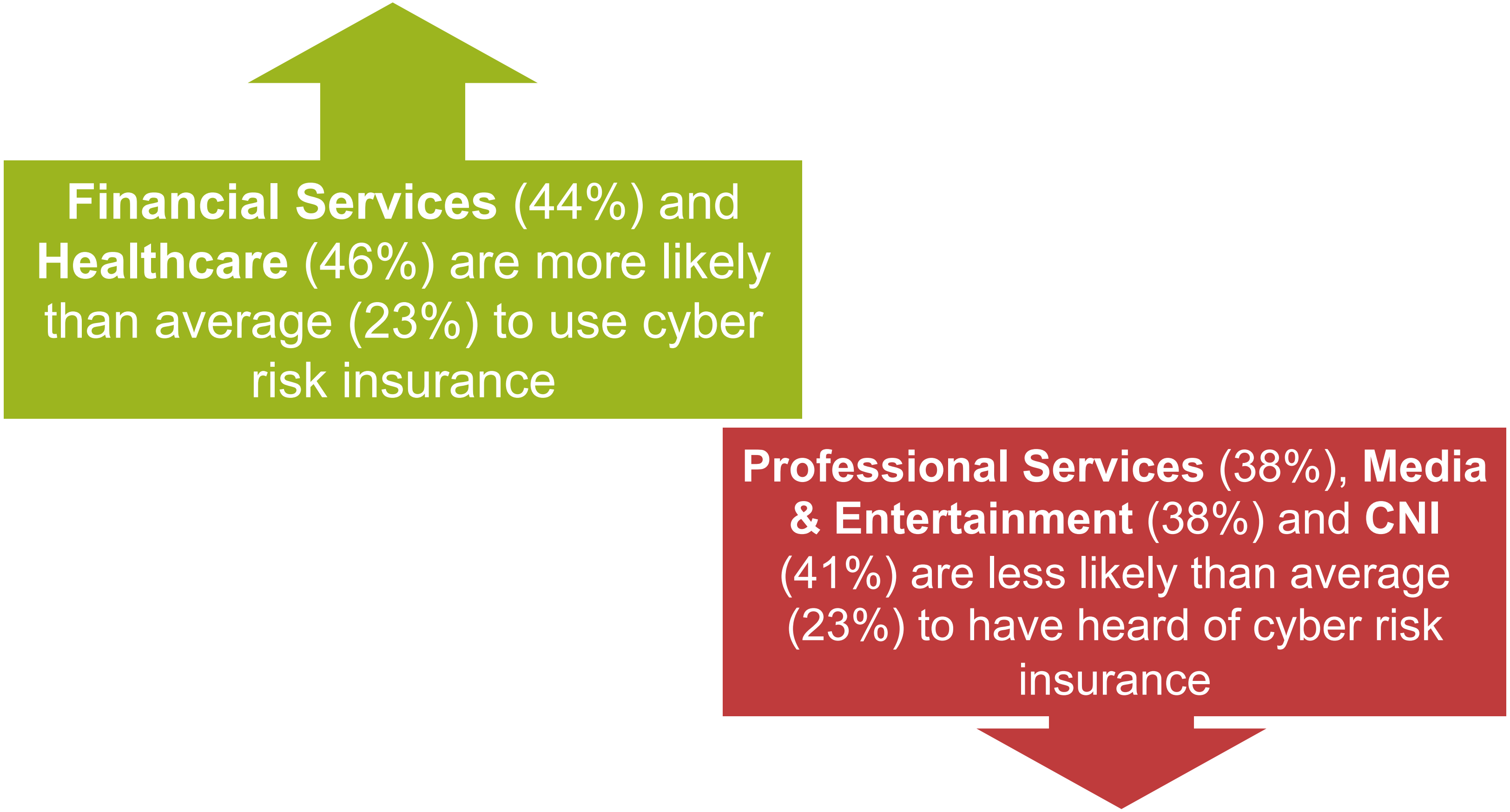
Are you using cyber risk insurance (also known as cyber liability insurance or cyber breach insurance)?



There are some interesting differences in cyber risk insurance awareness between IT and business executives. A substantially greater proportion of IT decision makers are considering using such insurance, but almost twice as many business executives have never heard of this type of insurance.

n=230

Industry View

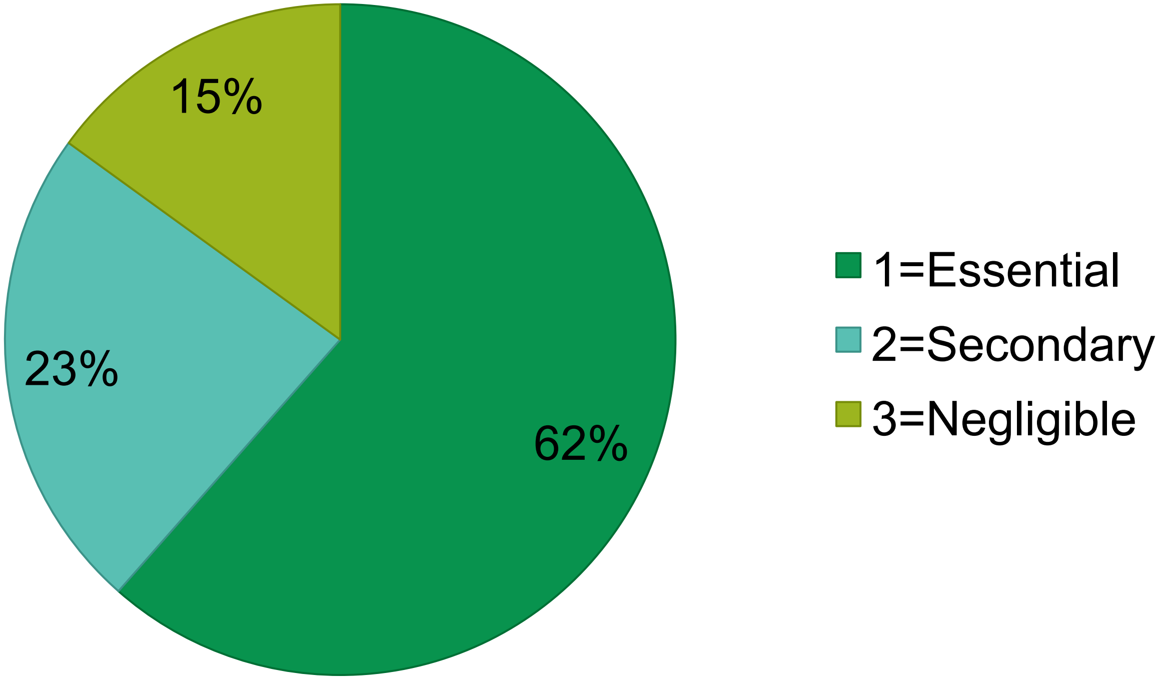


Financial Services (44%) and **Healthcare** (46%) are more likely than average (23%) to use cyber risk insurance

Professional Services (38%), **Media & Entertainment** (38%) and **CNI** (41%) are less likely than average (23%) to have heard of cyber risk insurance

5 Requirements on providers

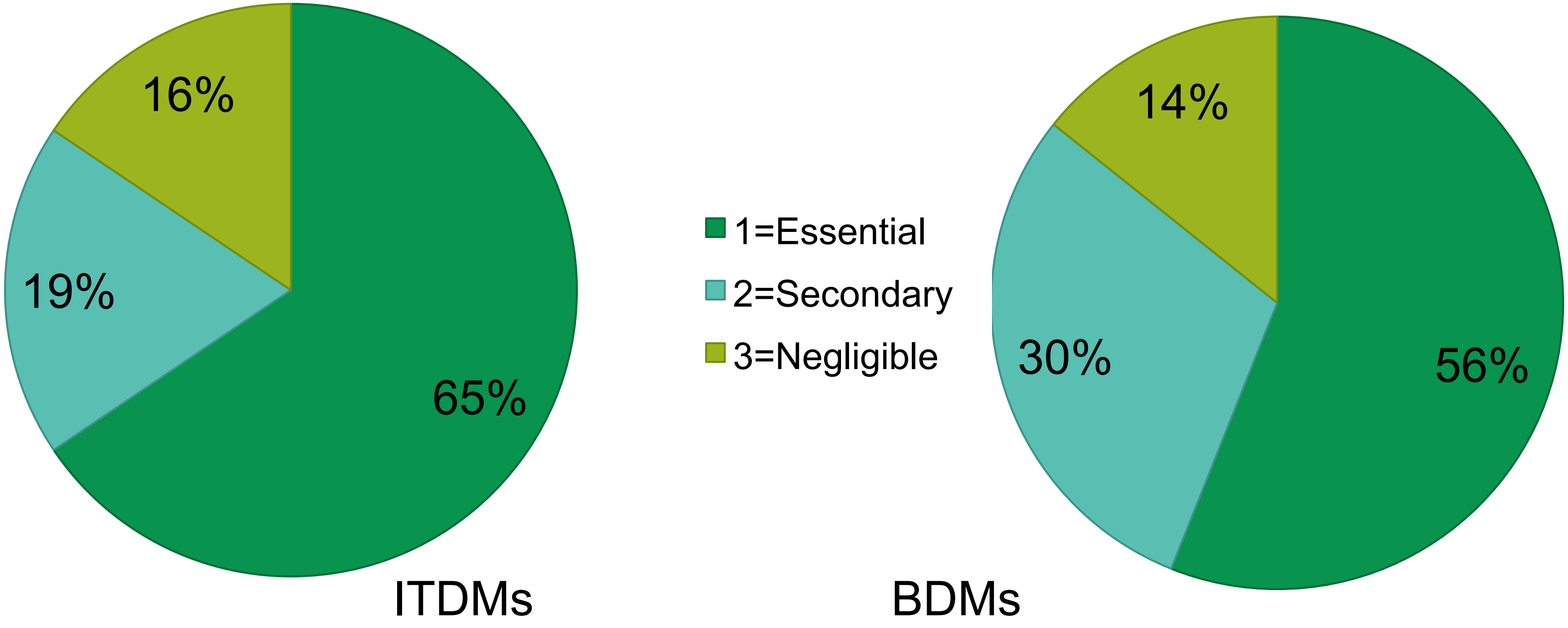
How important is it for your security providers to locate your data in the UK?



Data location and data sovereignty are often considered as important issues in cyber security, as it underpins data privacy. So we were interested to understand attitudes towards mandating data to be located in the UK, or whether companies were relaxed about physical location as long as their security needs will be met.
In fact, organisations care a lot about data location. Almost two-thirds of respondents said that it was essential for their security data to be located within the UK, even though there is no legal requirement for them to do so (in the vast majority of cases).

n=230

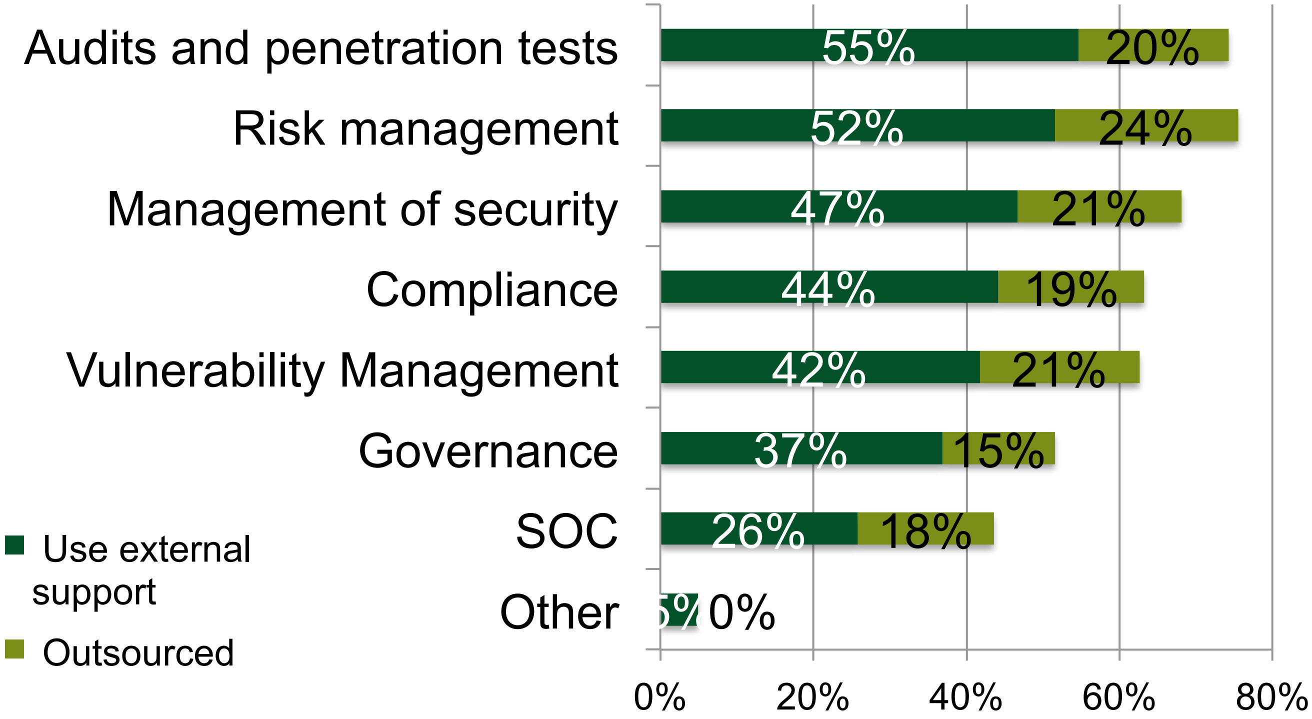
How important is it for your security providers to locate your data in the UK?



There is a clear split in the attitude towards data location between IT and business people. Business executives appear to be much more relaxed about UK-located security data than IT decision-makers.

n=230

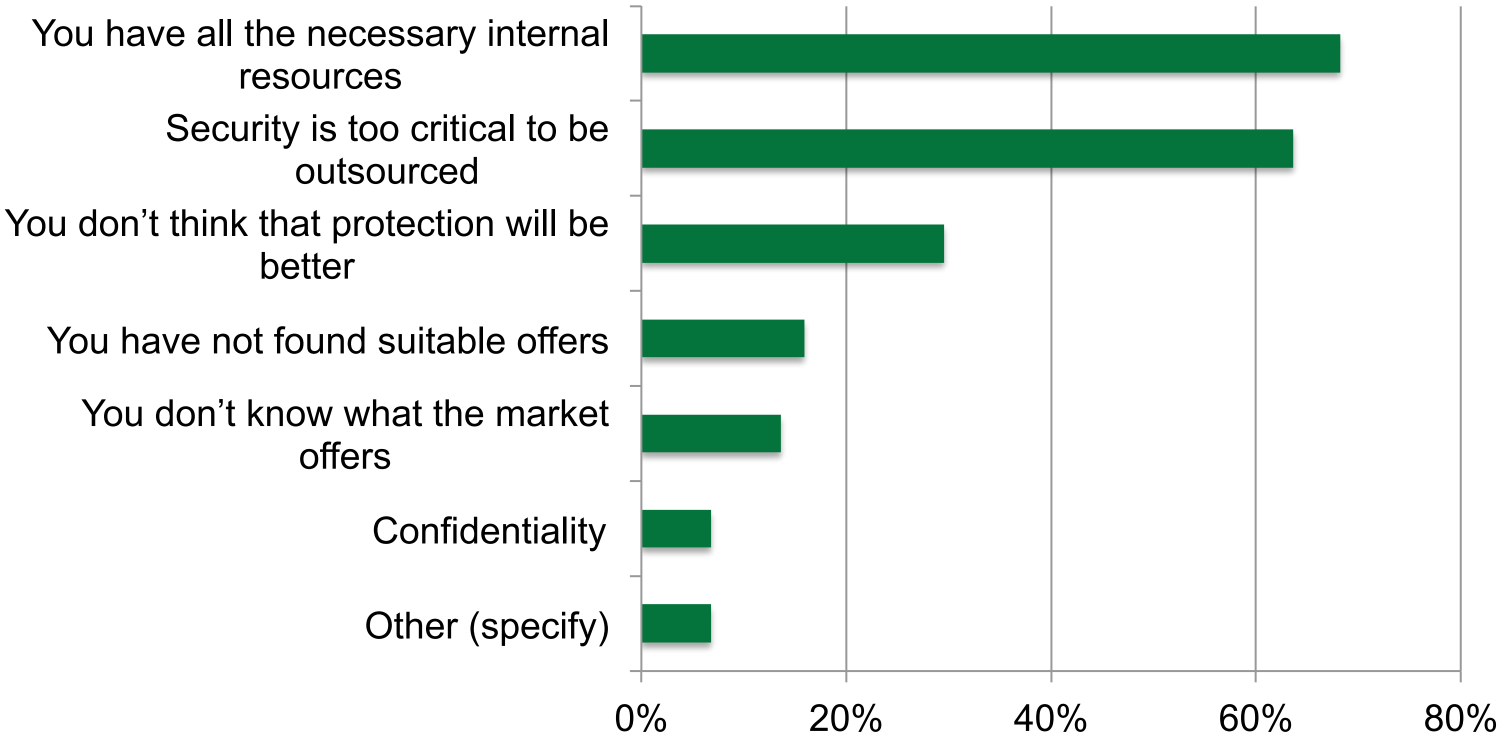
Which elements of your IT security have you used external support for, or have you outsourced? Select all that apply.



Of those organisations that currently outsource or use external support for security provision, a majority target risk management (combined 75%) and audit & penetration tests (76%). 68% of firms that use some external provision do so in the management of security solutions, a oft-reported headache for CISOs.

n=163

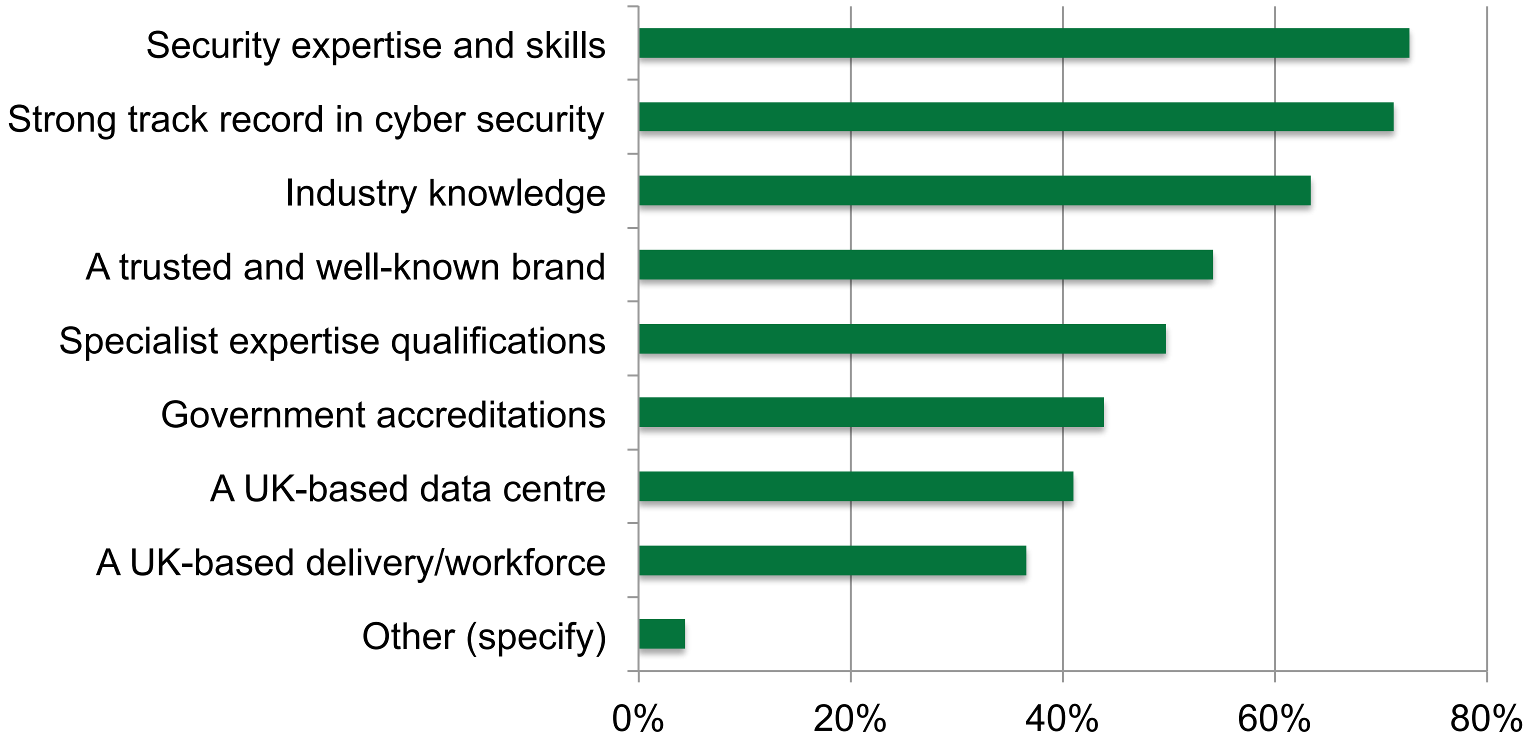
Why have you not outsourced ? Several possible answers



We were interested to understand why enterprises decide not to outsource. The overwhelming answer is that they have no perceived need to do so: two-thirds of organisations not outsourcing claim that they have all the necessary internal resources they need. In addition, a majority also believe that security is too critical to be outsourced, which echoes our earlier finding regarding a strong reluctance to outsource.

n=44

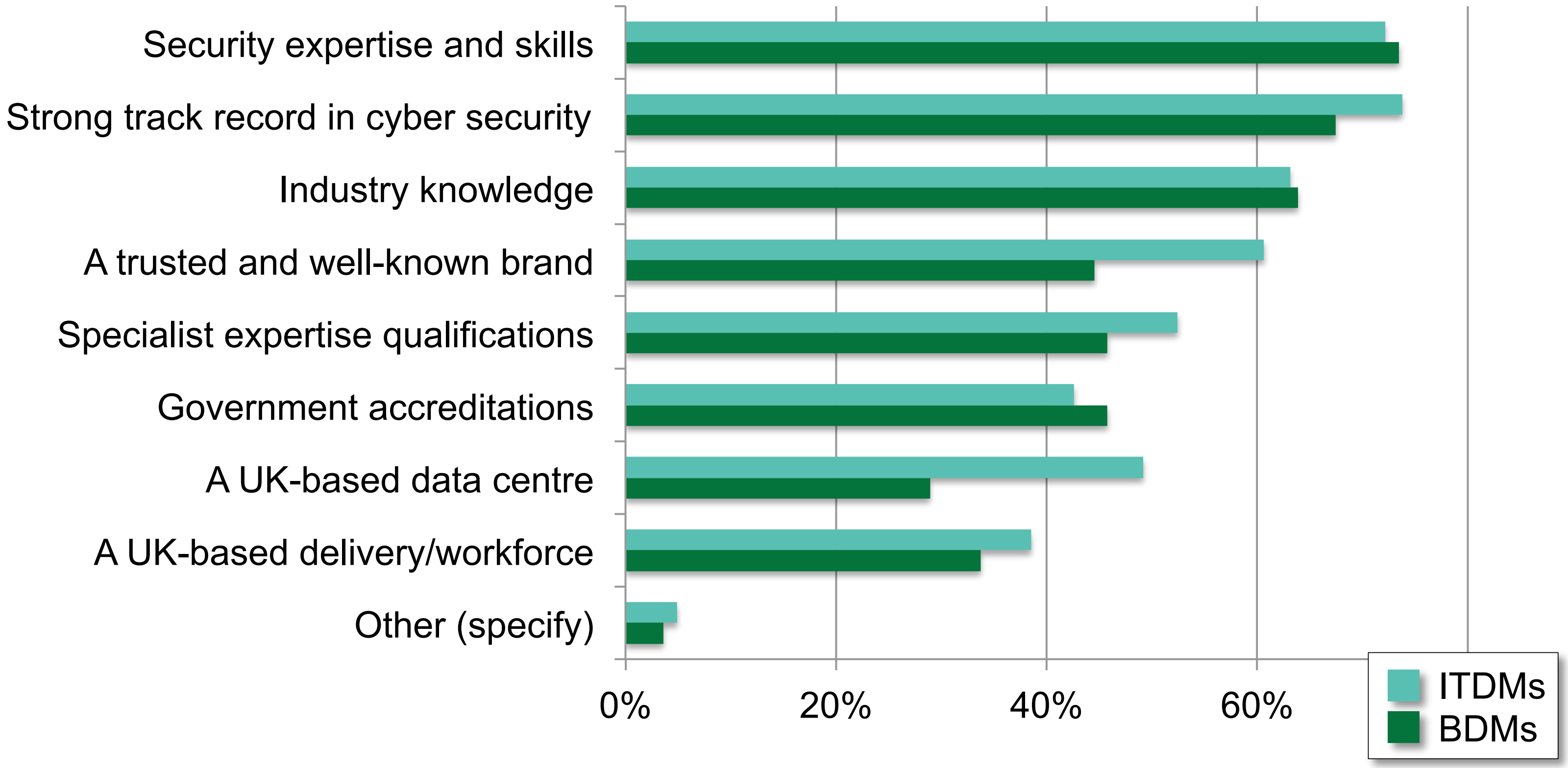
When considering a security services provider what do you look for?



Enterprises are clear when asked to report the key attributes of a potential cyber security services provider. They value evidence, in the form of a strong track record and security expertise and skills. Industry knowledge is also important, as is a trusted and well-known brand.

n=205

When considering a security services provider what do you look for?



Interestingly, IT decision-makers are much more concerned about the brand of a provider, and they strongly favour a UK based data centre. Business decision makers are much more relaxed about the physical location of data but they are slightly more concerned about industry knowledge.

n=205

Interim conclusion

Cyber security is **critical to organisations**. And although they currently use external providers, they are clear that when they do such providers must come with **robust credentials**.

Cyber security is too important to businesses for them to adopt additional risks with their suppliers. It is important then for suppliers to **communicate their track records**, and strong **industry knowledge** is also extremely useful.

6 Overall conclusion

Analyst conclusion (I)

Duncan Brown
Research Director, Cyber Security
PAC UK

Large companies in the UK **are under siege** from cyber security threats. A vast majority of executives see the cyber threat as increasing, including three-quarters of business managers. Cyber security visibility in the boardroom is also increasing, and workloads are rising in response. But **most organisations remain under fiscal pressures** and the majority are seeing no increase in their cyber security budgets.

Most firms are aware of the **scarcity of cyber security skills**, and although they would prefer to hire in permanent staff to boost their internal capability, they recognise that this is neither feasible nor affordable. Under a not insignificant degree of duress, companies use external providers to provide cyber security provision across a wide variety of areas. Use of external resources on individual projects is the most common way of procuring such services, but outsourcing is **more prevalent than most companies initially admit to**.

Why is this?

Analyst conclusion (II)

Duncan Brown
Research Director, Cyber Security
PAC UK

Companies are **reluctant to outsource** due to a collection of different reasons. Clearly, there is the tendency for executives to claim self-sufficiency in providing services internally. Few would readily admit to being unable to fulfil their operational responsibilities. Then there is the specific nature of security: it is one of those disciplines that companies worry about leaving to 3rd parties.

It is a comment on the state of cyber security industry that, despite these concerns, 79% of companies do (or plan to) use external providers for cyber security capability. We must conclude that, given the reluctance to use external providers, the fact that most companies are doing so means that they are **unable to cope** with the demands on internal resources.

Companies are ready to adopt a **cautious and selective approach** to outsourcing or the use of external resources for project-based work. This reflects a **pragmatic approach to the problem of budgetary and skills concerns**. Buying in external capability as and when needed makes sense, but for more long-term provision Managed Security Services are more likely to be deployed.

Disclaimer, usage rights, independence and data protection

The creation and distribution of this study was supported by Fujitsu Technology Solutions GmbH, among others.

For more information, please visit www.pac-online.com.

Disclaimer

The contents of this study were compiled with the greatest possible care. However, no liability for their accuracy can be assumed. Analyses and evaluations reflect the state of our knowledge in July 2014 and may change at any time. This applies in particular, but not exclusively, to statements made about the future. Names and designations that appear in this study may be registered trademarks.

Usage rights

This study is protected by copyright. Any reproduction or dissemination to third parties, including in part, requires the prior explicit authorization of the sponsors. The publication or dissemination of tables, graphics etc. in other publications also requires prior authorization.

Independence and data protection

This study was produced solely by Pierre Audoin Consultants (PAC). The sponsors had no influence over the analysis of the data and the production of the study.

The participants in the study were assured that the information they provided would be treated confidentially. No statement enables conclusions to be drawn about individual companies, and no individual survey data was passed to the sponsors or other third parties. All participants in the study were selected at random. There is no connection between the production of the study and any commercial relationship between the respondents and the sponsors of this study.

About us

From strategy to execution, PAC delivers focused and objective responses to the growth challenges of Information and Communication Technology (ICT) players.

PAC helps ICT vendors to optimize their strategies by providing quantitative and qualitative market analysis as well as operational and strategic consulting. We advise CIOs and financial investors in evaluating ICT vendors and solutions and support their investment decisions. Public institutions and organizations also rely on our key analyses to develop and shape their ICT policies.

Founded in 1976 and headquartered in Paris, France, PAC is part of the CXP Group, the leading European research & advisory firm in the field of software and IT services.

For more information, please visit: www.pac-online.com

PAC's latest news: http://blog.pac-online.com

Duncan Brown
Research Director,
Cyber Security

+44 (0) 20 7553 3966

d.brown@pac-online.com