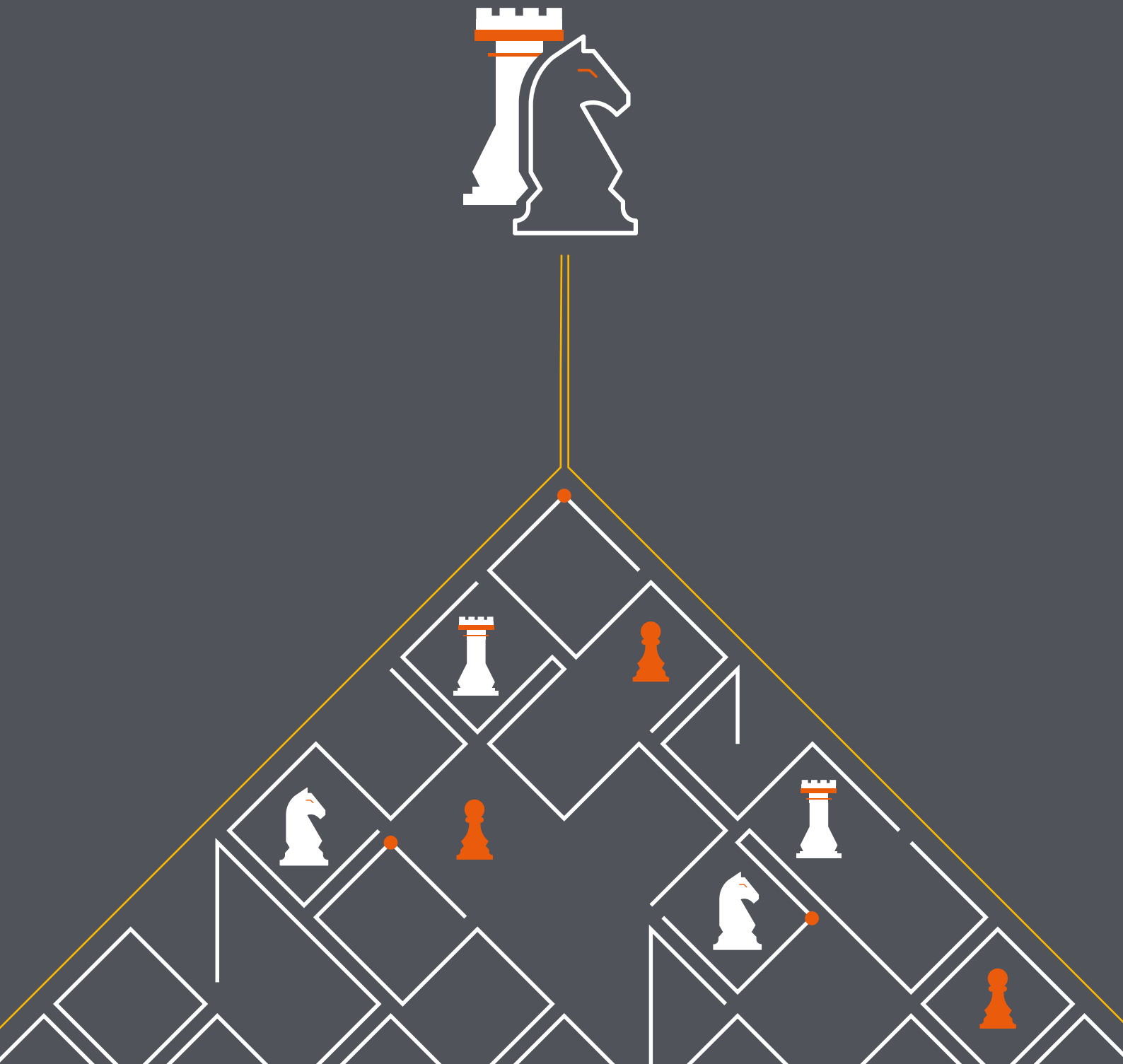
BAE SYSTEMS
INSPIRED WORK

The intelligence disconnect

The 2017 Cyber Defence Monitor: A global perspective



Foreword

Over the past few years, cyber security has steadily climbed up the business agenda. Today, putting the right protection and protocols in place to defend against cyber risk is now front of mind for senior leaders around the world.

Our business is committed to helping protect the many thousands of companies we work with from increasing cyber threats. We know that cyber criminals can take many different forms, each with their own motivations and methods of attack. For businesses, staying ahead of the evolving threats in an increasingly complicated landscape can be a real challenge.

We commissioned strategic insight analysts, Opinium, to undertake an extensive piece of research to understand the current state of play when it comes to business cyber security. We interviewed 221 Board level executives and 984 IT Decision Makers in eight markets around the world to understand their concerns and perceptions of preparedness when it comes to their own cyber security.

This research confirms the importance that business leaders place on the cyber security of their organisations. However, it also shows an interesting disparity between the views of our C-suite respondents and those of the IT Decision Makers. Both groups understand that they face threats, but their understanding of the nature of these threats and of the way they translate into business and technological risks can be very different.

While the businesses we spoke to have confidence in their cyber security measures, our research also shows that the majority of respondents expect the number and severity of cyber attacks to rise in the year ahead. To counter this, they plan to devote more time and resources to cyber security.

It is therefore vital that we plan for the future skills requirements of the cyber sector today, nurturing the talent we need to ensure a thriving sector, equipped to address a growing challenge.

Businesses also see increased knowledge sharing - with peers, law enforcement, governments or IT security firms - to supplement their defences against cyber crime. In an increasingly connected world, it is no longer possible for businesses to work effectively in silos.

> The research shows an **interesting disparity** of views between the C-suite respondents and IT Decision Makers

Partnerships such as the Joint Money Laundering Intelligence Taskforce and the National Cyber Security Centre in the UK, as well as the sorts of working relationships we build with organisations like the secure financial message provider, SWIFT, are paramount. It's clear that businesses benefit from collaborative efforts to understand and tackle the threats we all face today.

A diversity of opinion tied to common goals is a symptom of strength in an organisation. It's clear from our research that effective collaboration, communication and intelligence sharing are the bedrock on which effective defences will be built.

Kevin Taylor

Managing Director, BAE Systems Applied Intelligence

Executive summary

We surveyed two distinct groups within companies – C-level executives at Fortune 500 companies, and IT Decision Makers (ITDMs), asking them about their attitudes to risk and their understanding of the adversaries facing them, and how they marshalled their organisations' resources in defence.

Cyber security represents the most significant business challenge to 71% of C-suite respondents. Amongst ITDMs, 72% expect to be targeted by a cyber attack over the next 12 months.

There was a noticeable difference between the two groups when it came to all three of these areas. Perhaps more worrying: both groups believe the other is reponsible in the event of a succesful breach.

Close examination of the responses to our survey suggested that, while these two groups agree on many things, they often do so from very different perspectives, symptomatic of a lack of clear communication and agreed basic information shared between executives and IT leaders. In turn, this division shapes how and when companies go about defending themselves and, at the extreme, whether they are able to do so effectively.

This extended to the sorts of things the two groups worried about. Senior executives, charged with assessing and managing business risk, were worried about the theft of sensitive information and customers' personal data. In contrast, IT managers were concerned with a more broad set of potential losses, some of which were operational, but many of which reflected a more mature understanding of the consequences of a successful attack.

It is also notable that the two groups differed in their assessment of the cost of an attack: C-level executives estimated $11.6 million, while IT Decision Makers averaged out at $19.2 million.

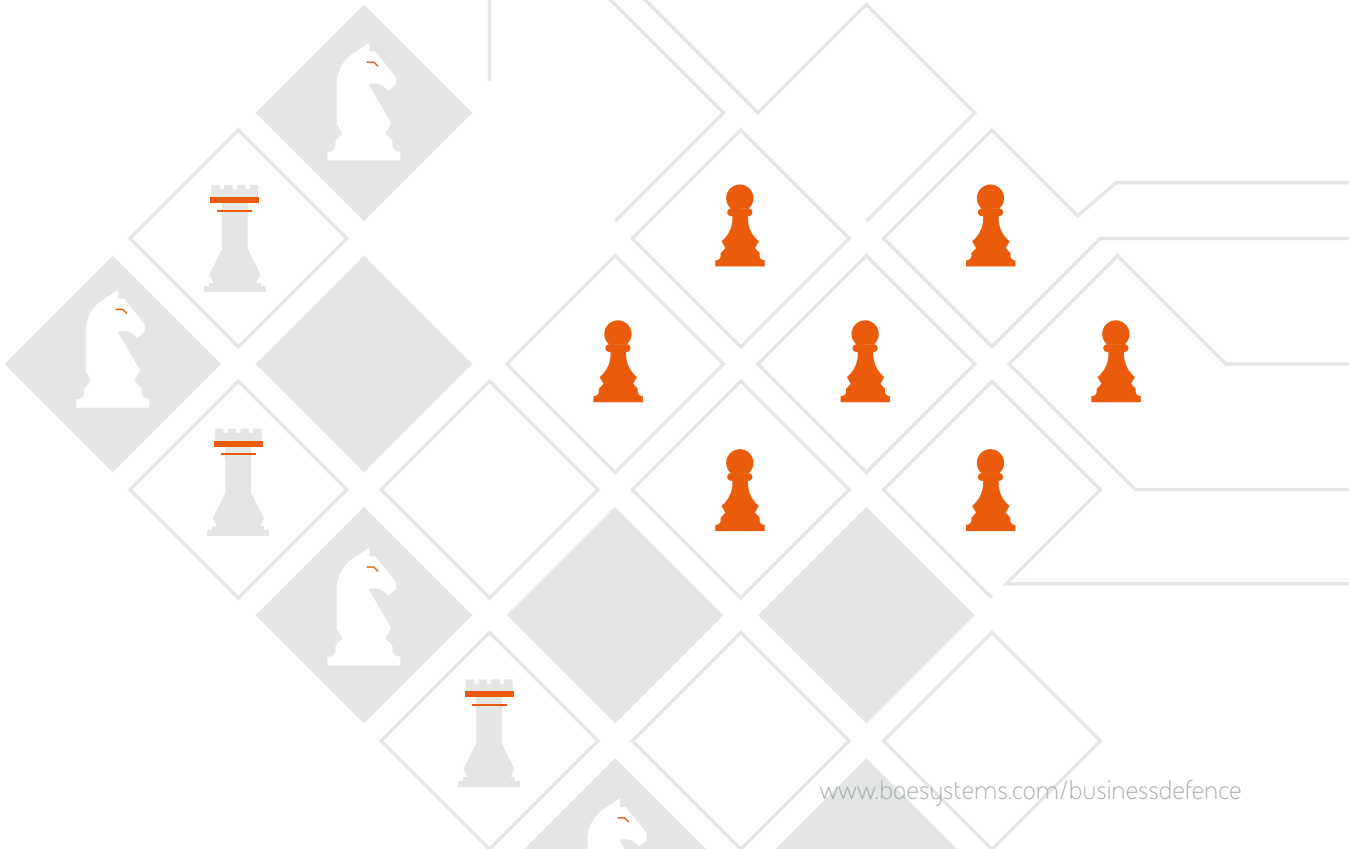
In both groups, confidence in their organisations' defences against cyber attack was very high. Our research revealed that businesses are increasingly aware of the unpredictable nature of the cyber threats they face. Businesses are increasingly aware of the unpredictable nature of the cyber threats they face, and, despite differences, C-suite executives and ITDMs alike are taking increasingly pragmatic and informed choices about how they go about minimising the risks they face.

The cost of a cyber attack by C-level executives is estimated at $11.6 million, while IT Decision Makers estimate $19.2 million

C-suite

While these two groups agree on many things, they often do so from very different perspectives

ITDM



CHAPTER I

The intelligence disconnect

We just don't talk any more

Our survey shows that while the concerns of IT Decision Makers and C-suite respondents are generally aligned, there are still gaps between how these two groups think. Sometimes it's down to differing perceptions of the same thing. At other points, it's the result of very different levels of experience.

ITDMs and business leaders don't always communicate openly, directly or comprehensively. This information gap is not solely due to different priorities.

ITDMs and C-suite respondents report different concerns in the event of a successful attack.

Business leaders are more worried about sensitive information theft, loss of customer information and reputational damage. ITDMs are more worried by Intellectual Property (IP) theft, fraud and business disruption.

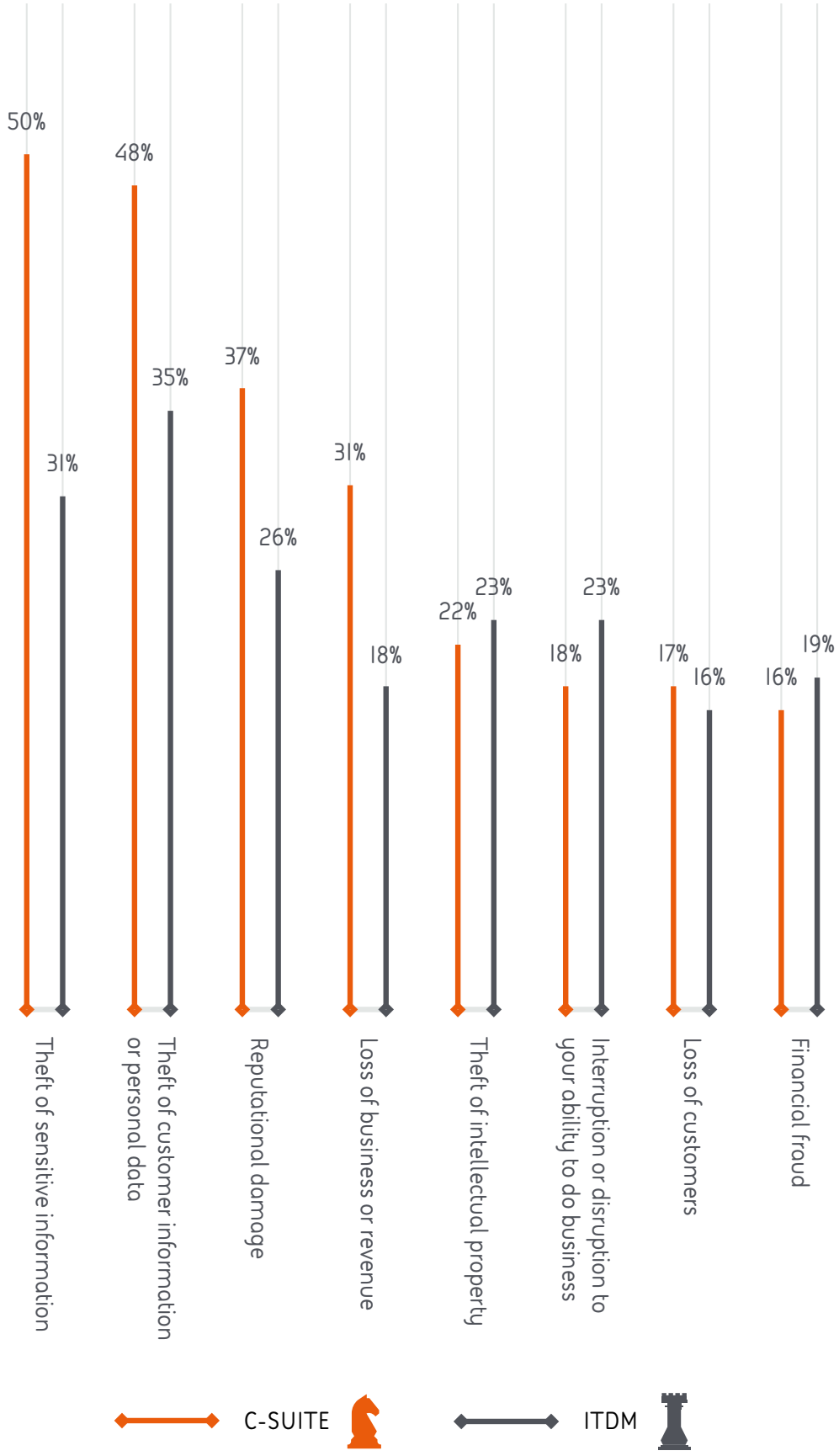
Half of the executives we spoke to feared losing sensitive information, but for the ITDMs, this is secondary to the loss of personal data and other customer information. Quite rightly, ITDMs are more concerned than executives about an attack interrupting or disrupting their organisation's ability to do business: after all, their focus is at the operational level in the event of an attack.

While the C-suite's responses presented more of a consensus, it's also interesting that ITDMs had a far wider variety of concerns, giving a more even spread of responses. Put simply, C-suite respondents tended to worry about the same threat. ITDMs, on the other hand, had much broader concerns.

This isn't adversarial

Our research indicates that this disconnect is not the cause of discontent; ITDMs feel supported and believe they have the right information to tackle cyber threats. Overall, **79%** of ITDMs said their organisations' Board of Directors took the risks associated with cyber attack seriously. Just over three quarters **(76%)** felt they had enough information to make informed decisions on cyber security and **73%** felt they had sufficient support from suppliers, enforcement agencies and government to tackle cyber risk. It's more probable that, because the two groups have different priorities, their perceptions of the same issues are directed by what they are looking to do: mitigate business risk or deliver effective IT that supports the aims of the business.

Half of executives fear the loss of sensitive information, but for ITDMs, this is secondary to the loss of personal data and other customer information

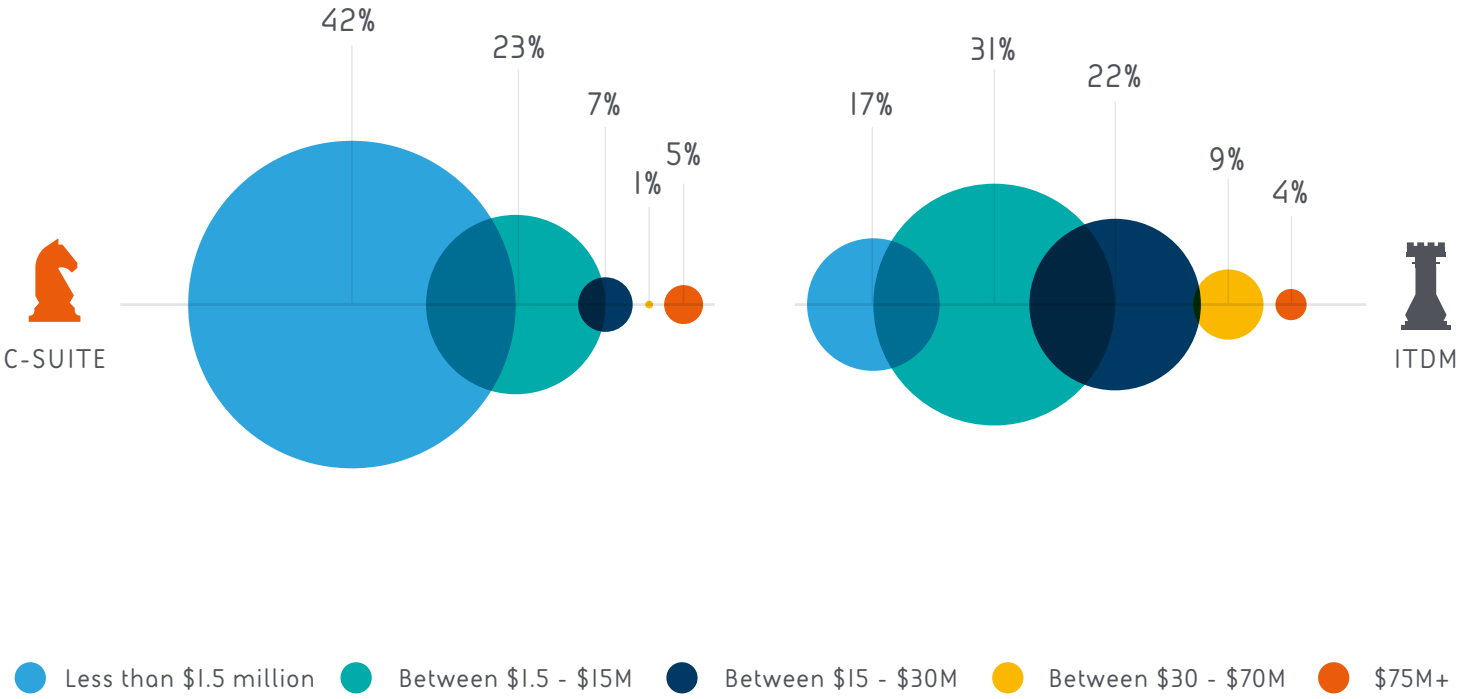


BIGGEST CONCERNS OF A SUCCESSFUL CYBER ATTACK

Successful attacks cost money

There was also a disparity in how much C-suite respondents and ITDMs expected a successful attack to cost them. We'll come to this in the next chapter, but it's worth noting that 42% of C-suite respondents expect a successful attack to cost them $1.5 million or less.

The potential financial cost of a serious, successful cyber attack on the business is estimated at $11.6 million according to executives and $19.2 million according to ITDMs

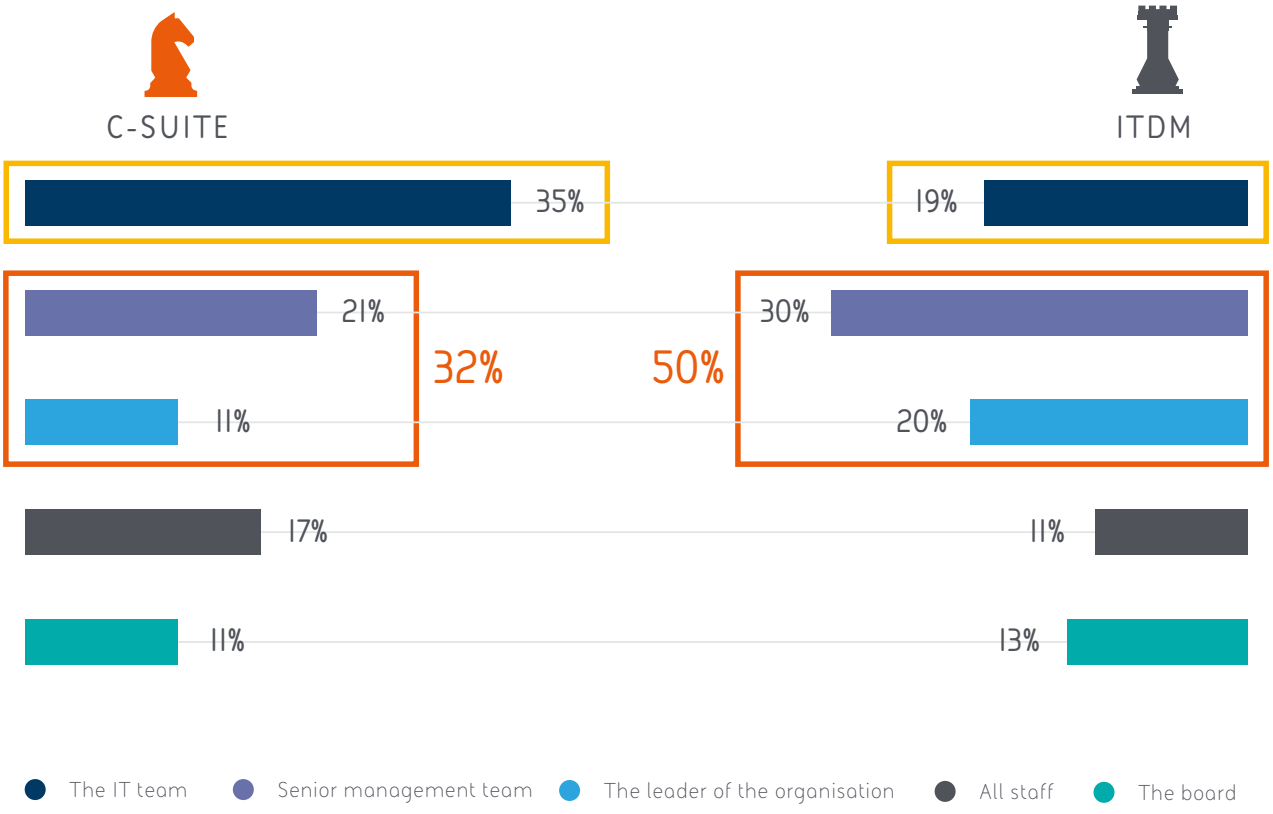


Who is responsible? Who is accountable?

Perhaps the biggest difference of opinion over is who is to blame in the event of a successful attack. We've already seen that both groups expect human error by employees to be the root cause of a successful attack, but responsibility for the failure of security is where, perhaps understandably, the C-suite and ITDMs point the finger at each other.

According to the business leaders we talked to, the IT team is ultimately responsible in the event of a security breach. ITDMs who responded to our survey thought senior management should shoulder the burden.

There's something going on here: is it possible that our respondents are dividing out responsibility from accountability? While the Board of a company and its IT director, may ultimately be accountable in the event of a successful attack that was not prevented because they were negligent, it is entirely possible for others to be held responsible. The well–meaning, well trained employee who clicked on what looked like an innocent link, in an innocent email, should not be held accountable. But they can be held responsible.



WHO IS RESPONSIBLE FOR SECURITY BREACHES?

So what?

The divergence of opinions between C-suite and ITDMs when it comes to potential threats, accountability and responsibility creates gaps for attackers to exploit. Such disconnects and communications failures can also create problems in the event of an attack, when time is often of the essence and clarity is important.

It's vital that organisations work to narrow these gaps in understanding, intelligence and responsibility.

CHAPTER 2

Counting the cost

Our research shows there is, again, a significant disconnect when it comes to how much ITDMs and C-suite respondents imagine the cost of a cyber attack on their organisation to be - with those in the C-suite seemingly underestimating its far-reaching effects.

Perhaps because they are closer to the detail when it comes to the volume and calibre of potential threats, as well as the security measures in place to combat them, ITDMs estimate the potential financial cost of a serious, successful cyber attack on their organisation to be $19.2 million.

By contrast, C-suite respondents estimate the cost to be much lower, at only $11.6 million, with a sizeable 42% of those expecting costs to amount to less than $1.5 million. This compares to only 17% of ITDMs, who seem far warier of the potential repercussions of an attack.

Our own experience suggests that these figures can be below the actual costs. C-suites and ITDMs should be careful to make full, informed assessments of the threats facing them, the risk of a successful attack, and the consequent costs of restoration and repair (see page 14).

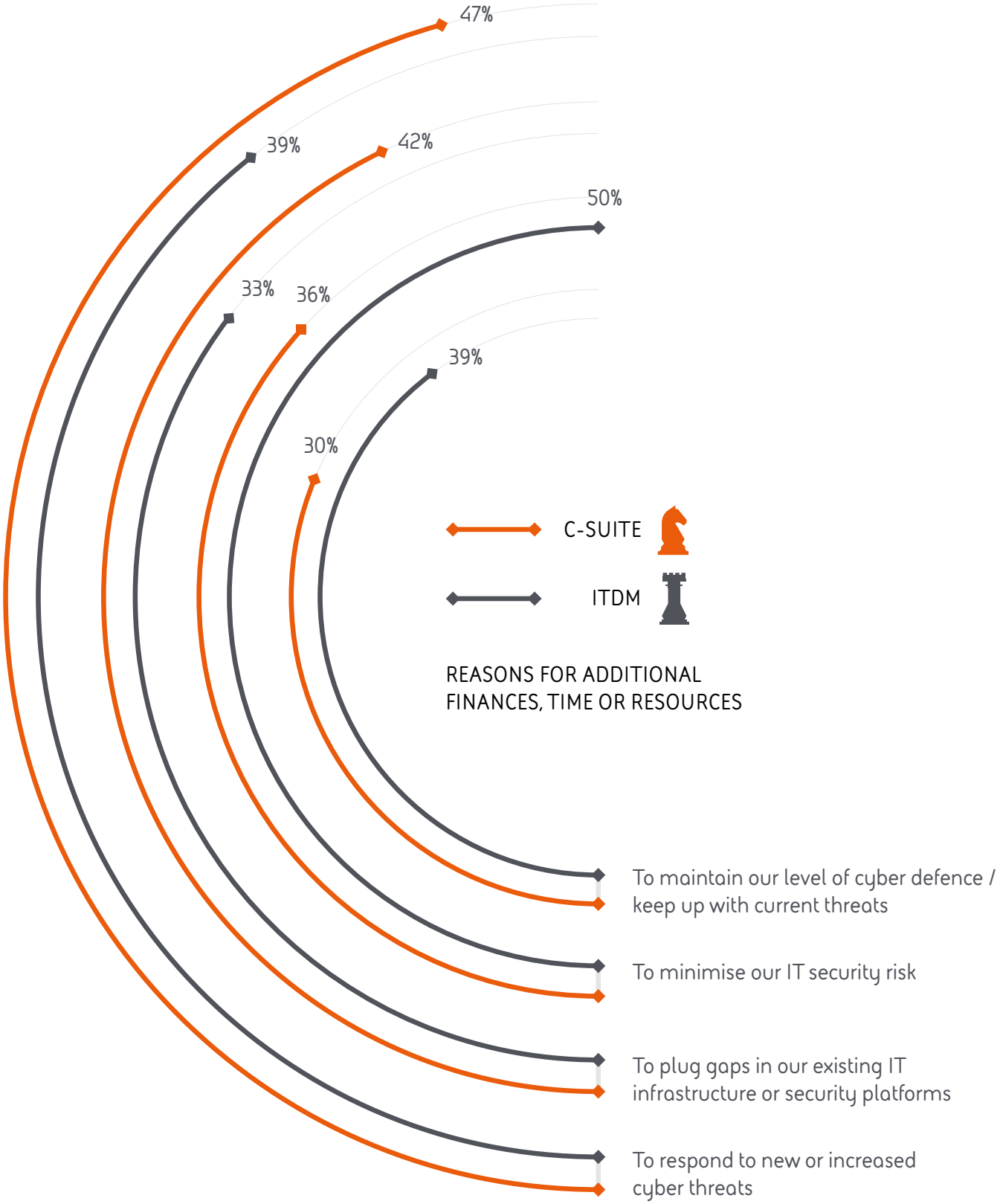
Perceptions of the cost of a successful cyber attack can also affect the amount businesses spend on cyber defence. Organisations may feel like they are investing adequately given the risk as they see it. We cover this in more detail in Chapter 3.

Ten to fifteen per cent of the IT budget is spent on cyber security with that figure set to increase, according to half of ITDMs. What's more, 82% of ITDMs believe this spend to be part of a comprehensive cyber security strategy, compared to only 50% of C-suite respondents.

Forty-one per cent of C-suite respondents believe the investment is more ad-hoc, perhaps because they have less sight of individual defence strategies and how these are working together as a whole for the business. This is a worrying indication that C-suite respondents seem to think their IT managers simply don't have as much of a cyber security strategy as they actually do. Closer examination of one particular question in the survey bears this out.

While 42% of business leaders thought additional resources were going on plugging gaps in infrastructure, compared to 33% of ITDMs, half of ITDMs and 36% of C-suite respondents said additional resources would go towards minimising IT risk – a far more strategic goal. While the overall figures (see illustration - right) suggested a relatively low difference of opinion, when the numbers are examined on a per-country basis, the two groups diverge violently in their thinking. For example, only 22% of C-suite respondents in the USA expected new resources to be directed to reducing IT security risk, compared to 56% of ITDMs. In Australia, 80% of C-suite respondents expect this to happen – compared to 46% of ITDMs. Clearly, the two groups have very different perceptions on whether resources are directed as part of a larger plan, or spent patching leaks in the dam.

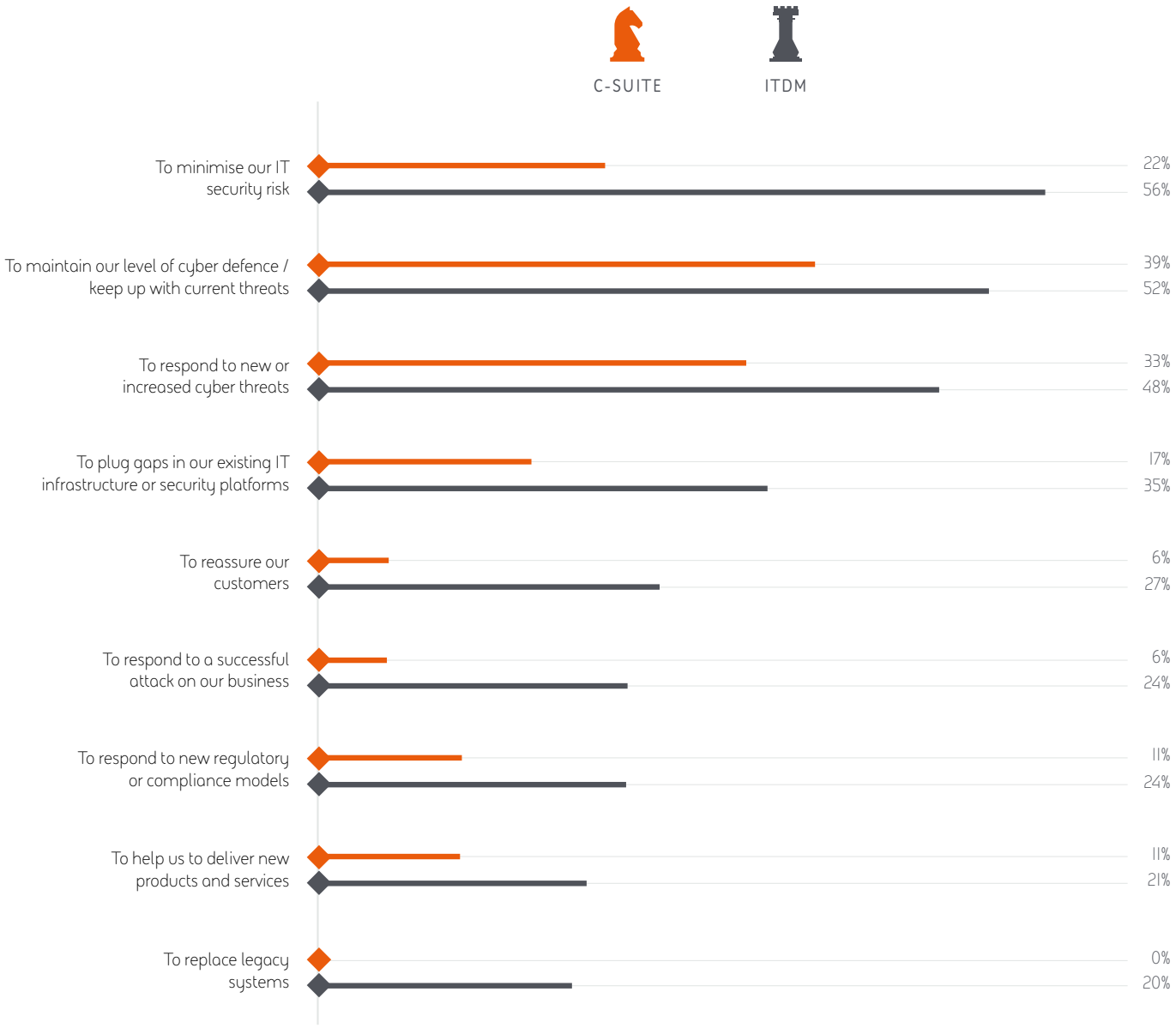
ITDMs estimate the potential financial cost of a serious, successful cyber attack on their organisation to be **$19.7 million**


47%
39%
42%
50%
33%
36%
39%
30%
C-SUITE
ITDM
REASONS FOR ADDITIONAL FINANCES, TIME OR RESOURCES
To maintain our level of cyber defence / keep up with current threats
To minimise our IT security risk
To plug gaps in our existing IT infrastructure or security platforms
To respond to new or increased cyber threats

REASONS FOR ADDITIONAL FINANCES, TIME OR RESOURCES - AUSTRALIA

An in-depth understanding of the company's cyber defence strategy is vital if executives are to assess and combat the risks effectively, especially since they may be directly accountable for any breaches that follow. We go into more detail on this in Chapter 3.

Smaller suppliers simply can't **defend** themselves as well, which starts to make them **attractive** to attackers



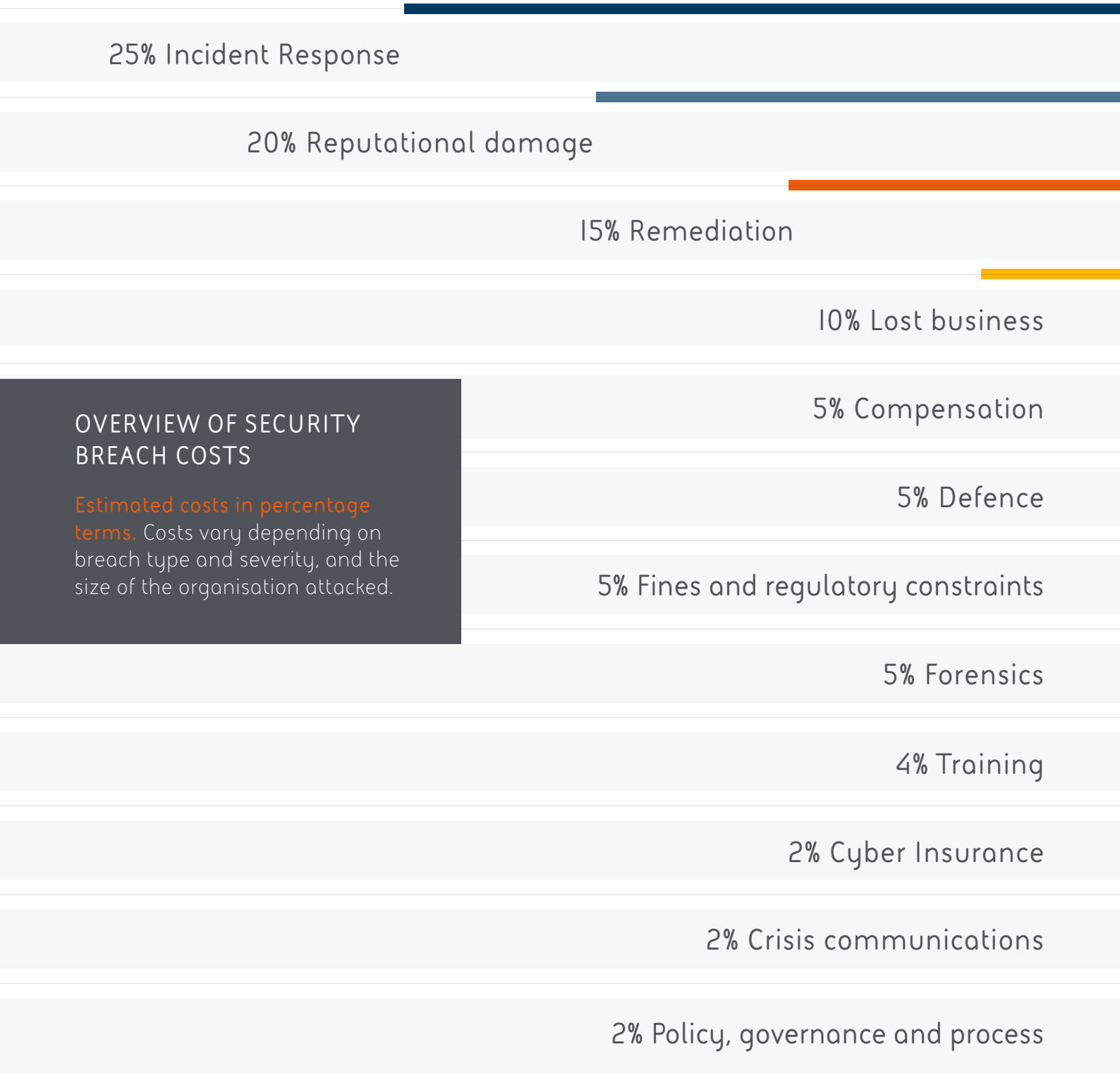
REASONS FOR ADDITIONAL FINANCES, TIME OR RESOURCES - US

Investment of time and resources in cyber security is set to increase in the coming year, according to both the ITDMs and executives we surveyed, in order to keep pace with new threats, minimise risks and plug gaps in existing IT infrastructure or security platforms. All of this requires security staff to update their skills regularly, and employers to both nurture existing staff and add to their team. In cyber security particularly, it can be difficult for smaller organisations to keep pace with this demand – and, for that matter, remain competitive in the recruitment market. This is a compounding problem for many organisations. Big companies can stay current, but their smaller suppliers simply can't defend themselves as well, which starts to make them attractive to attackers as relatively poorly protected entry points to their customers' networks.

It's nearly impossible to estimate the cost of a generic attack: there are simply too many variables before, during and after a breach, to do anything other than pull together aggregate or average. What might be more practical is to work out what the main areas of cost are likely to be. Our respondents were optimistic about costs, with 42% of C-suite respondents and 17% of ITDMs estimating the cost of a successful attack at less than $1.5 million. We asked people who would probably know: our team of security consultants, who are regularly called in by companies that have fallen victim to a breach. They explained why this might be the case:

OVERVIEW OF SECURITY BREACH COSTS

Estimated costs in percentage terms. Costs vary depending on breach type and severity, and the size of the organisation attacked.



What is a data security breach?

A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual or group unauthorised to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property. The 'real' costs to the business will come from the 12 key areas below and vary by size of business and the volume and type of data stolen.

Our survey suggests both IT and business leaders see the cost of a breach as being higher than the accepted figure. With regulatory fines starting to become a bigger issue for a larger number of organisations, organisations need to understand the likely costs they will have to shoulder, plan ahead for successful incidents and, again, ensure that the C-suite and ITDMs are comparing notes. This multi-million Dollar gap in expected costs suggests the communications problems we mentioned in the first chapter also apply to the impact of successful attacks.

How much it costs an organisation – in both internal and external expertise by the day, week or month – to deal with a confirmed security breach.

An area of a business which may not be fully understood or translated into financial terms, the loss of future business terms in the short, medium and long term.

The running cost of having everything needed to return the organisation to good health and back in business as quickly as possible - all ready and regularly tested. Remember: it's a case of when, not if, a breach will occur, so a plan is vital.

This includes expected business in the short term, current clients and customers. But it also includes longer term 'trust' of future business beyond the 12-18 months business horizon and publicity fall out 'window'.

Another area of business neither approached nor fully understood in financial terms. It will often be necessary to compensate customers for the costs they've incurred and loss of their data. Supplier and client organisations will also need compensating for business loss and Intellectual Property loss, or inability to deliver a product or service.

Monitoring and Detection. Organisations recognise that the longer it takes to detect and / or contain a security breach, the more dramatic the cost to the organisation.

Possible fines for loss of personal data and financial information and other data. There's also the added cost of increased regulatory compliance and audit placed on an organisation by regulators, regulations and government.

The cost of an internal or external forensic resource to deal with the Incident Response plan of a breach. A team will have to deliver a Forensic Readiness Plan and test it, and provide training for First Responders and associated support.

Future training: either required by the business or by a government body, client or regulator.

A breach can lead to increased premiums and excess costs, or caveats to current and future cyber insurance polices, including limiting acceptable and insurable risks.

There's a cost for dealing with the public relations fallout of a successful breach, as customers, partners, law enforcement and regulators pronounce upon the impact.

Ongoing or post-attack costs associated with creating clear policies and plans, governance and strategy planning. This involves IT governance, the IT Decision Makers, Risk and Audit committees. Finally, the appointment of a Chief Information Security Officer or Chief Data Officer responsible for data security.

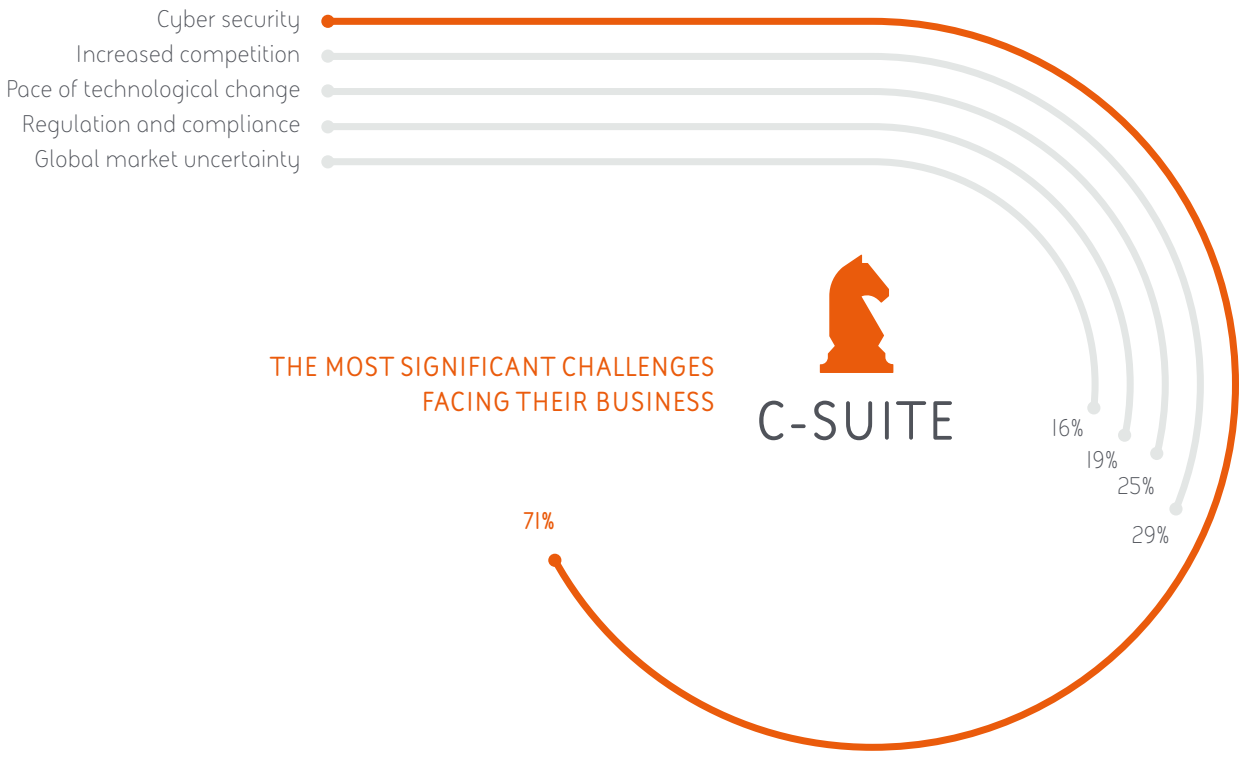
CHAPTER 3

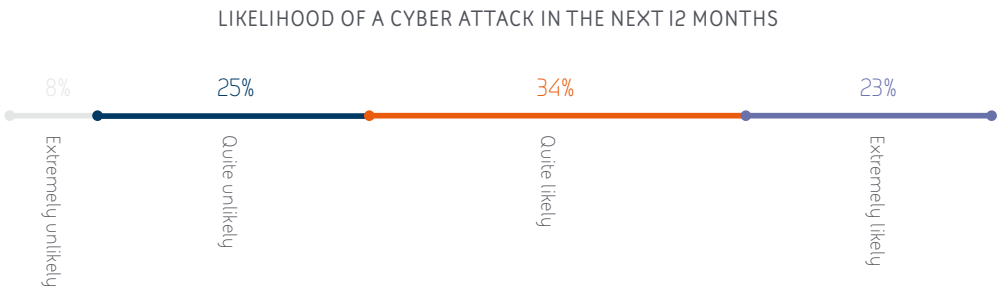
Confidence in defence

Cyber risk can be a subjective issue. Understanding risk, and dealing with it, is part and parcel of running an organisation. Understanding how organisations across the world feel about the risks associated with a cyber attack gives insight into both how they run and the threats they worry about.

Our research shows that cyber security is regarded by both ITDMs and business leaders as being in the top three challenges their businesses face today. It's clear that this topic is considered to be of massive importance to both managers of business risk and those who concern themselves directly with cyber risk.

Our respondents believe cyber security is one of the top three challenges their organisation faces

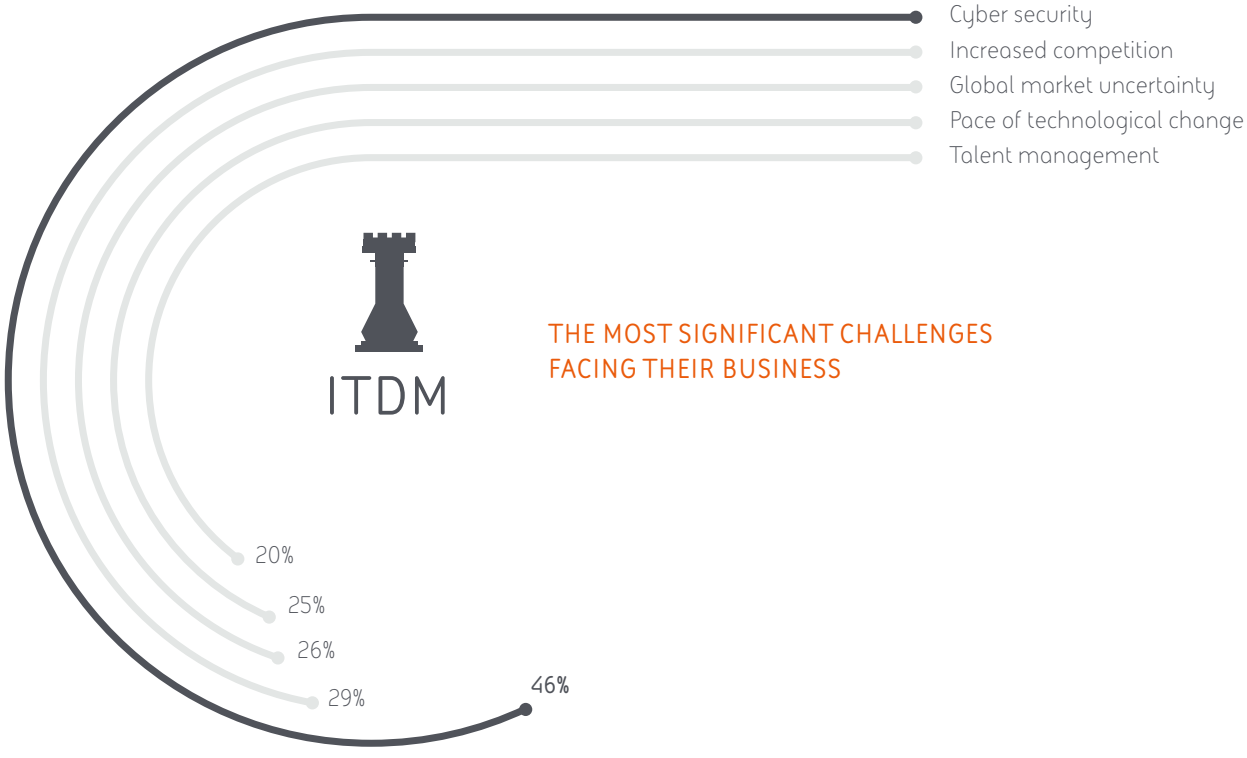


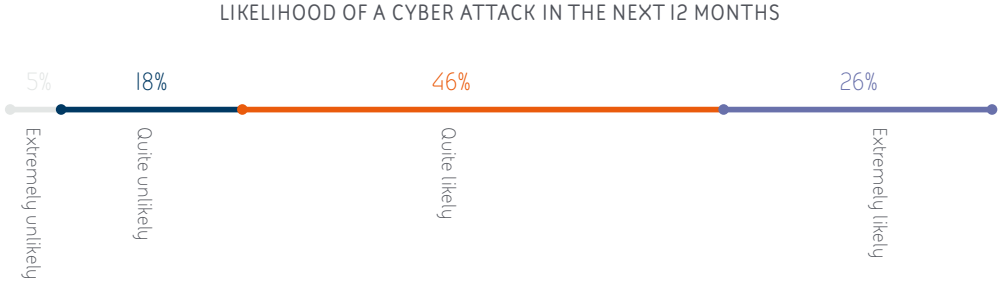


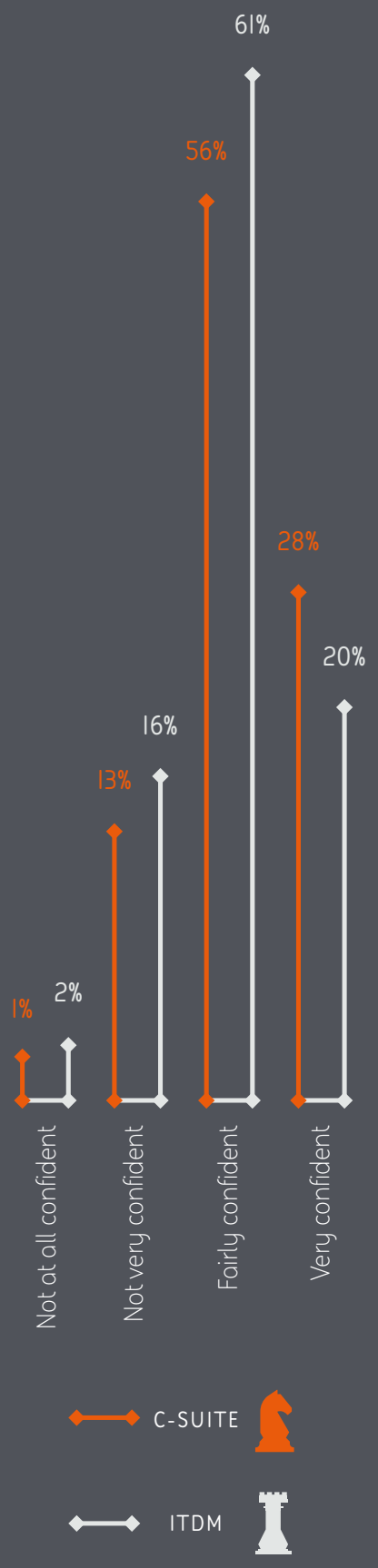
Organisations feel they'll be targeted

Understanding the scope of the threat one faces is difficult. Business and IT leaders feel overwhelmingly that a cyber attack targeting their organisation in the next year is either extremely or quite likely. Amongst the countries we surveyed, German ITDMs were most confident their business wouldn't be targeted, while those in the UK and Malaysia were least confident of escaping the attentions of a targeted attack. In Australia, business decision makers were the most pessimistic, with 73% thinking an attack was likely – compared to Germany, where only two in five C-suite respondents expected to be attacked.

Organisations think they can prevent these attacks: the overwhelming majority of respondents had high confidence that their business was well-equipped to repel attack. The story varies a little between countries; for example, executives in Singapore seem pessimistic about their chances, with 14% saying they were not at all confident their organisation could fight off an attack.







CONFIDENCE THAT YOUR BUSINESS IS WELL EQUIPPED TO PREVENT AN ATTACK

Maximising your cyber spend

Perhaps one reason for this level of confidence in one's defences is that many organisations have diverted a large proportion of their resources – cash, people, time and training – towards fending off cyber attacks. As we saw in Chapter 2, business leaders believe that a tenth of their organisation's IT budget is spent on cyber security and defence. Among ITDMs, this figure is 15%.

Our accident-prone employees are very well trained

Despite confidence that their people know to do the right thing, many of our respondents expected that human error by an employee would be the reason an attack on their business would succeed.

A full 70% of C-suite respondents and 83% of ITDMs say they are confident that their employees adhere to security procedures. The same groups cite human error on the part of the same employees as the reason why an attack would succeed – to the tune of 64% of business decision makers and 32% of ITDMs. This raises an interesting question. The training's valuable, but equally, C-suite respondents expect their employees to make mistakes despite it, and let attackers in. ITDMs seem more trusting – yet even so, a third of respondents also expect human error to result in a successful attack.

As we've said before, this appears to be a disconnect of sorts. In fact, it may also simply be the acceptance of human nature. Even the best trained, most astute and conscientious employee can fall victim to social engineering.

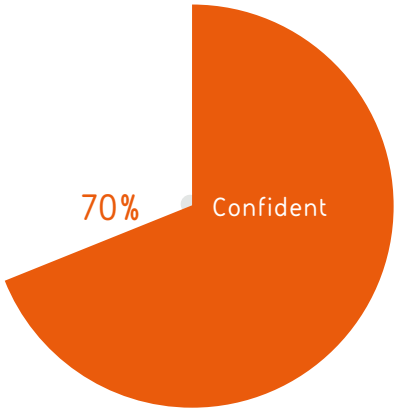
What does this all mean?

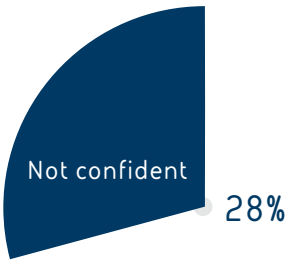
Companies expect to be attacked – but they're confident they can defend themselves for two reasons: they've spent money on their defences and they've trained their staff to identify and defend against cyber threats. The danger in this is that companies can develop a siege mentality, where confidence in one's defences leaves one blind to a weak spot.

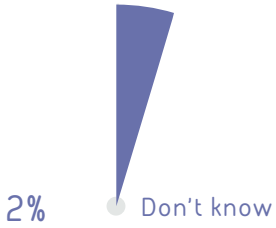
There is a huge degree of confidence in the defences businesses have put in place – despite a universal expectation that the sophistication and volume of attacks will continue to increase. A forward looking, strategic approach to cyber defence is important to stay ahead. Bearing in mind the very different views we've already seen the two groups in the study express, it's also vital that clear communication between board and IT department is both created and maintained.

CONFIDENCE THAT EMPLOYEES ADHERE TO SECURITY PROCEDURES

C-SUITE

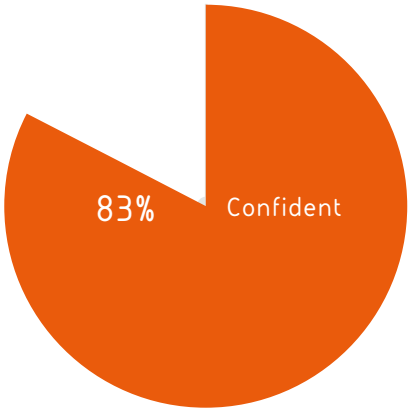


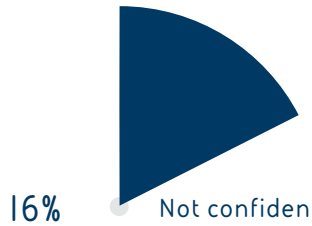


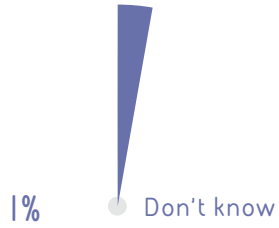


CONFIDENCE THAT EMPLOYEES ADHERE TO SECURITY PROCEDURES

ITDM







CHAPTER 4

Detecting the threat

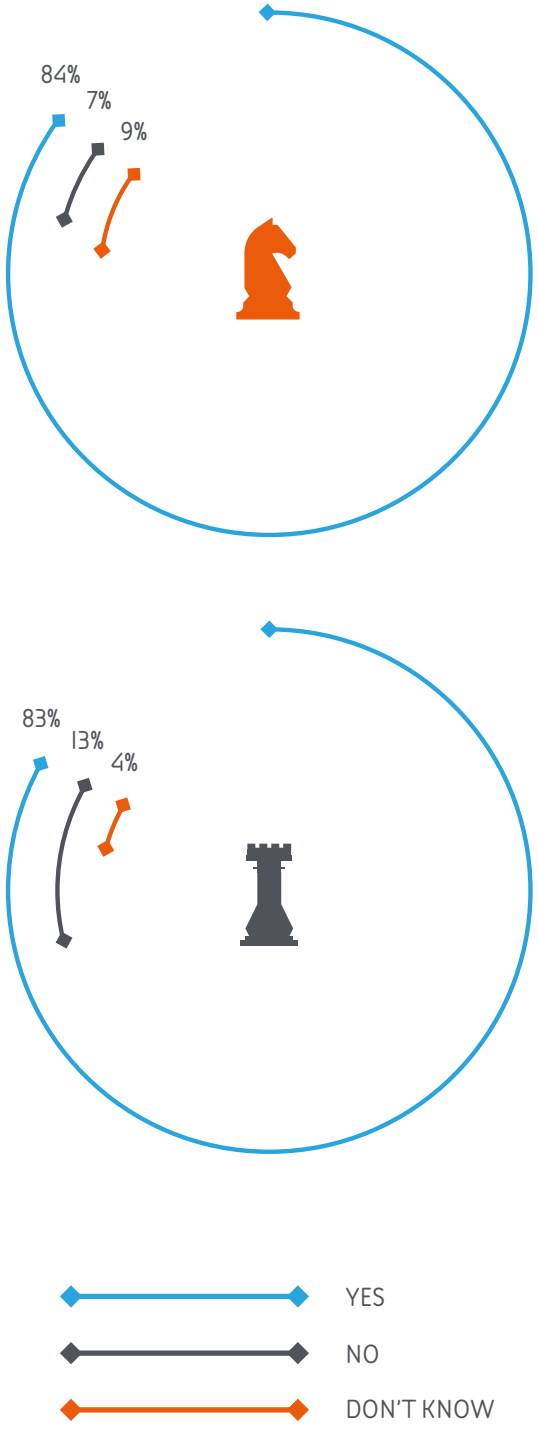
Many of our respondents gave evidence of an entirely level-headed approach to understanding the threats they face: they have some form of SOC to manage their cyber security risk.

Security Operations Centres (SOCs), both within an organisation or provided as a Managed Security Service (MSS) monitor security alerts and threats, and are common among the organisations we surveyed, demonstrating that most businesses are taking the issue of cyber security seriously, and that C-suite executives and ITDMs are aligned on the need for them.

It can be easy to mistake more alerts for more attacks – and conversely, interpret an alarm that does not sound as evidence of a lack of threats

Eighty-three per cent of ITDMs say they have a SOC within their organisation, with over half (51%) saying it forms part of their overall IT team or infrastructure. Meanwhile, just under a quarter (24%) say they have a dedicated SOC and 7% say it forms part of another team or part of the organisation.

Both ITDMs and C-suite respondents confirm that the level of alerts these teams are seeing is on the rise. This naturally varies from company to company, and the volume of automated, scattergun-style attacks by professional crime gangs is more than likely to create more alerts. But when even minor changes to the parameters of security monitoring devices and software agents can create massive, fresh volumes of alerts, it can be easy to mistake more alerts for more attacks – and conversely, interpret an alarm that does not sound as evidence of a lack of threats. A further interesting question to pose within organisations may be the extent to which their security teams see the nature of the threats and attacks they face evolving.

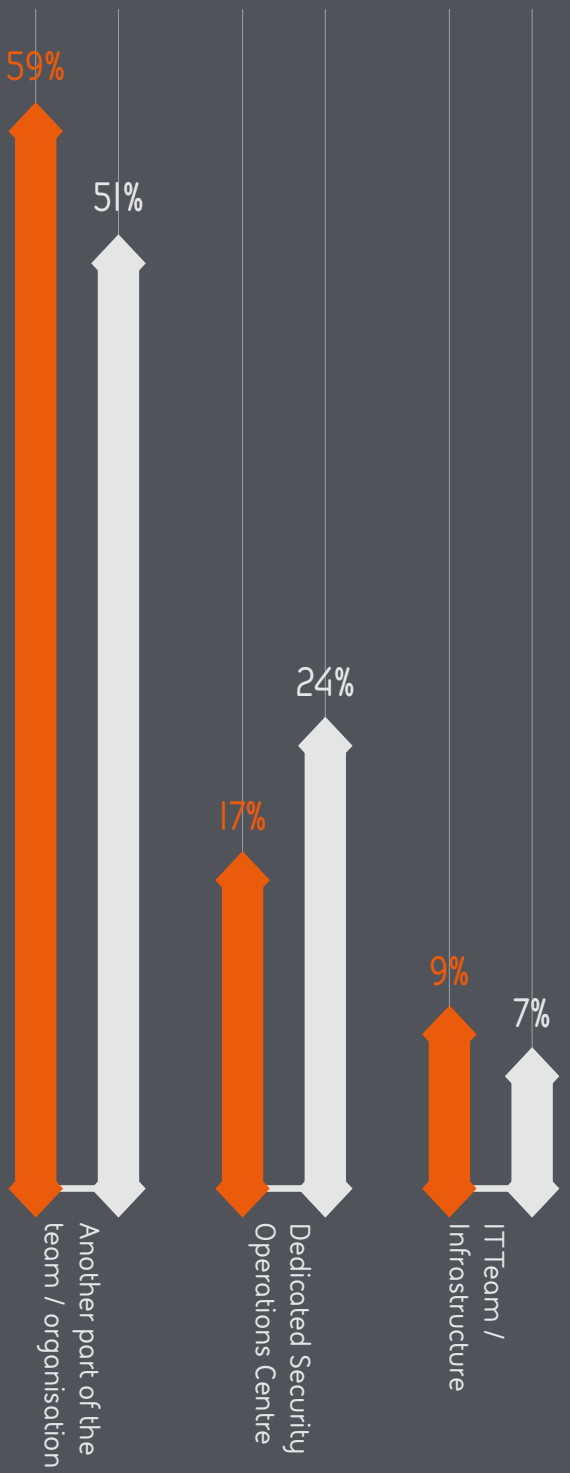


DOES YOU ORGANISATION HAVE A SECURE OPERATIONS CENTRES (SOC)?

TEAM THAT MONITORS ALERTS AND THREATS

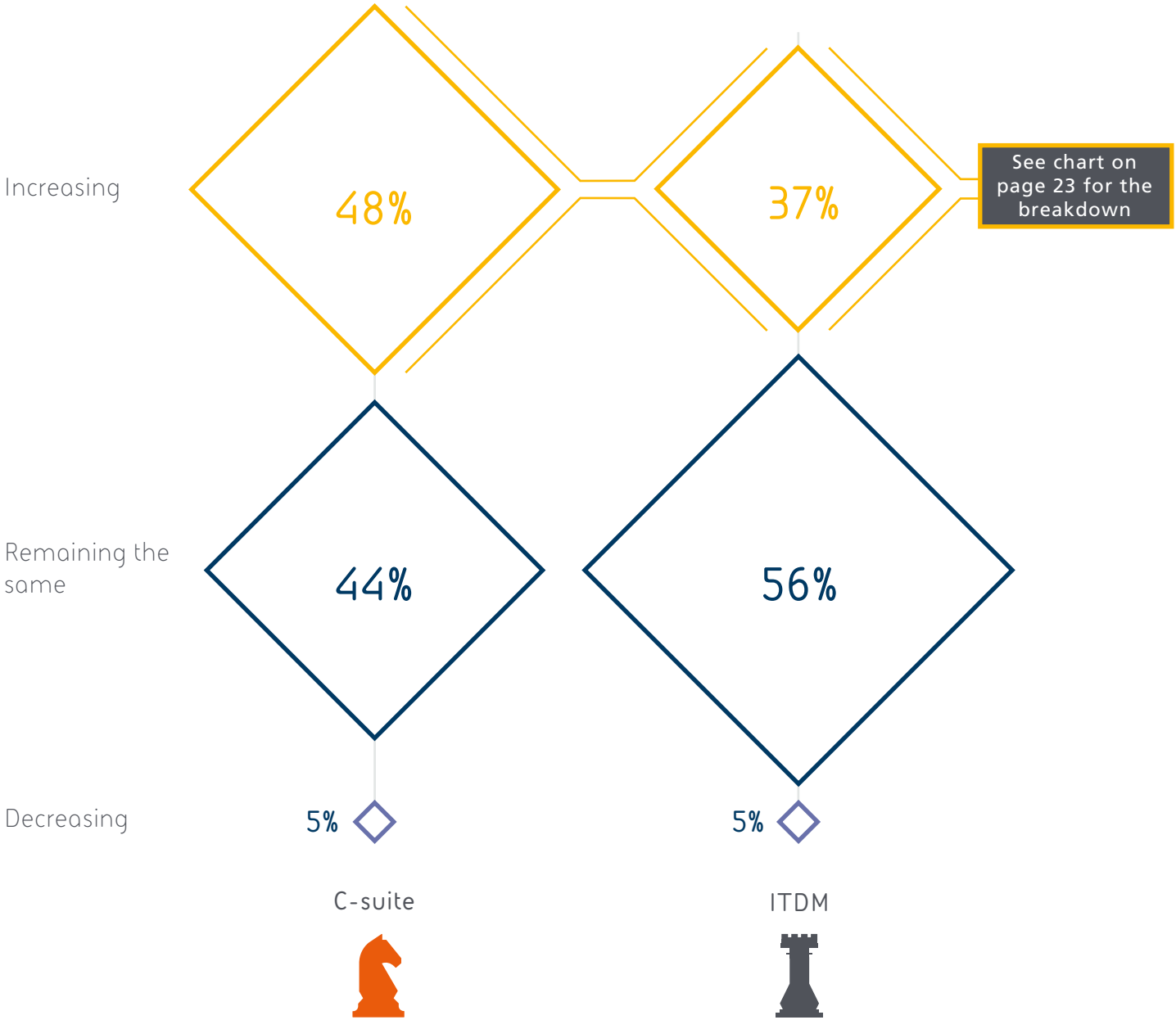
C-SUITE

ITDM

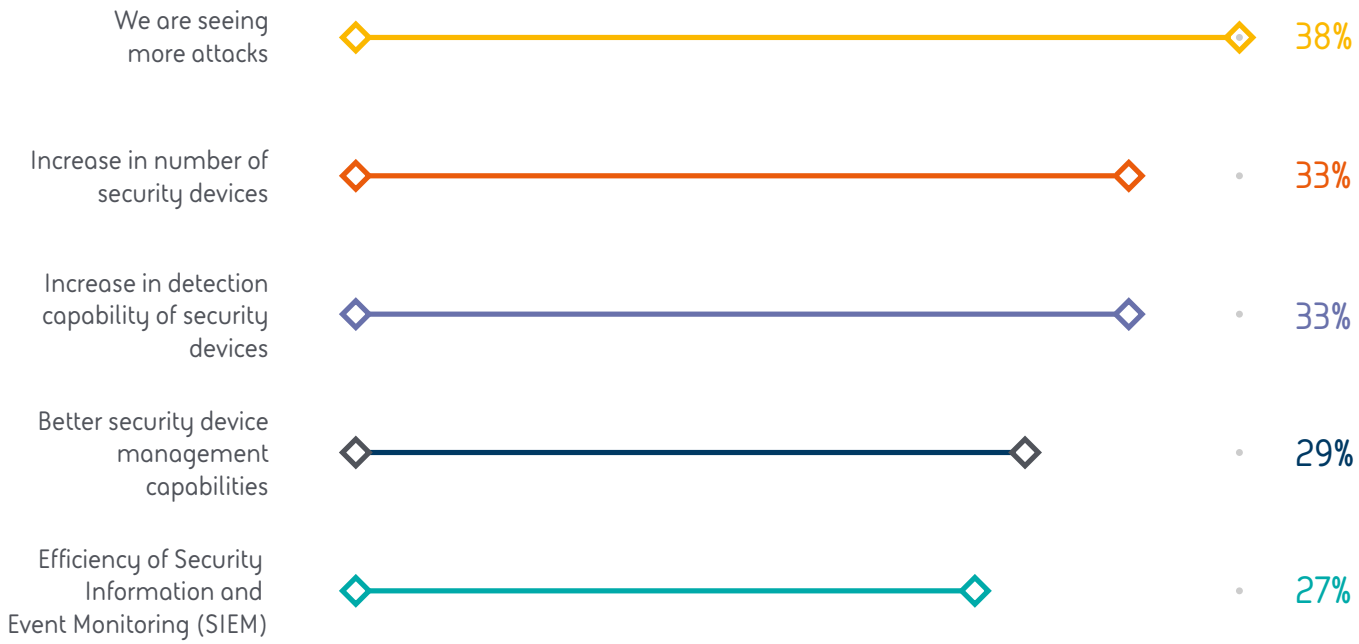


ITDMs are more likely than C-suite executives to think their business will be targeted by a cyber attack

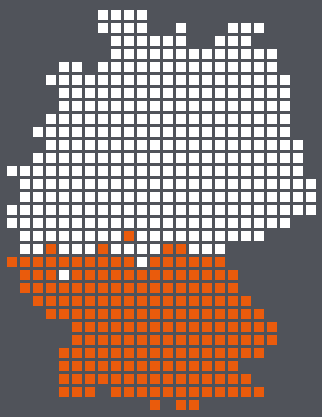
A third of ITDMs (33%) report an increase in both the number and detection capabilities of security devices at their disposal, while 29% cite better security device management capabilities



ARE ALERTS INCREASING?

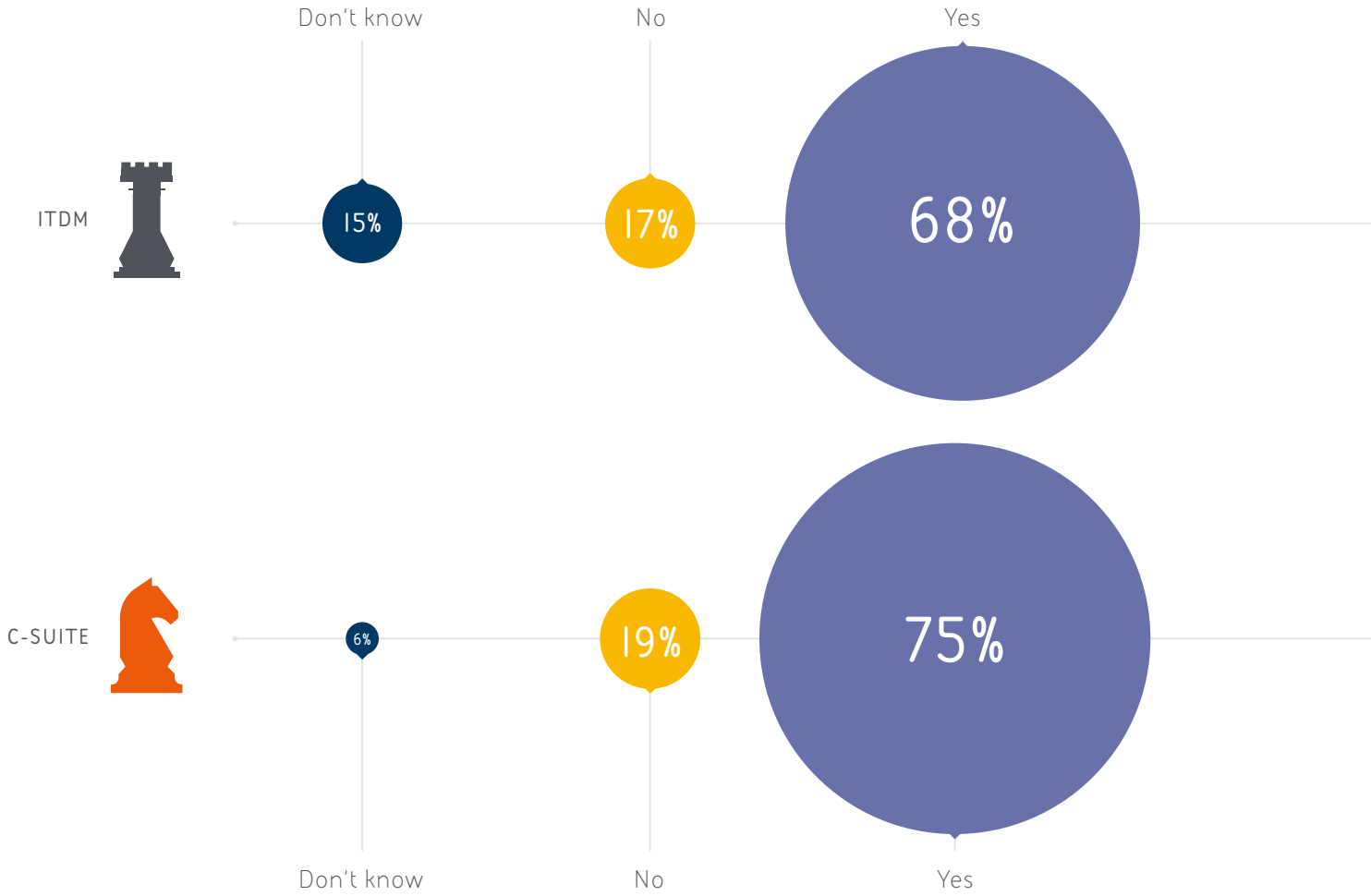


REASONS FOR INCREASED ALERTS



Australian C-suite workers are most wary with 73% thinking an attack is likely compared to just 40% in Germany

German ITDMs are the most confident that they will not be attacked (32% responded 'unlikely')

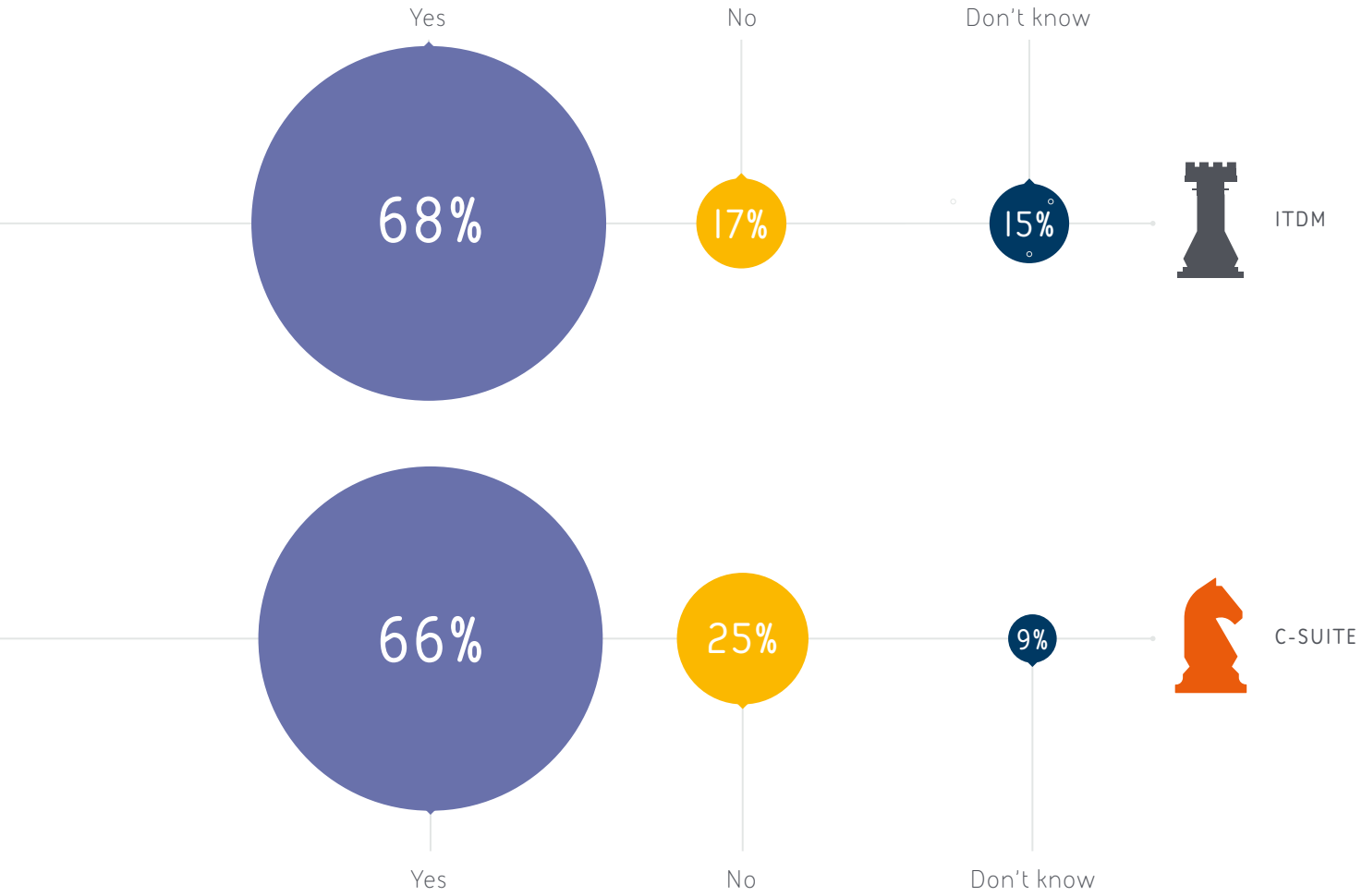


DO YOU THINK THE NUMBER OF CYBER ATTACKS WILL INCREASE NEXT YEAR?

The majority of ITDMs (68%) and C-suite respondents (75%) expect the number of attacks they see to increase in the coming year. What's more, around two thirds of ITDMs (68%) and C-suite workers (66%) believe the severity of attacks will increase as well.

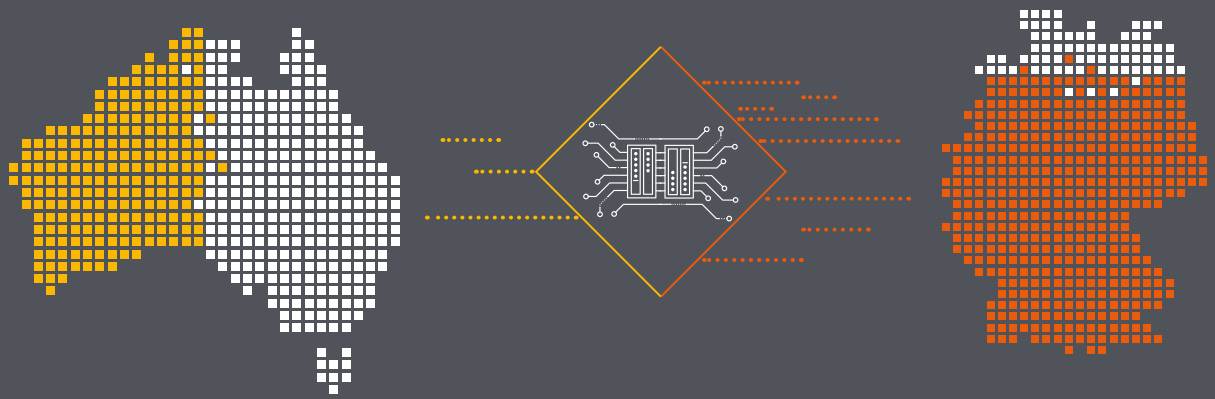
A SOC of some kind will help organisations manage their cyber risk. However, it shouldn't be a tick box – all sides agree the volume of attacks is rising, and this also raises issues of increases in attack sophistication and managing this growth without becoming swamped with alerts, data and attacks. Organisations must regularly update their SOCs (and their people's skillsets) and engage outside organisations to help.

Meanwhile, there is a **significant** disconnect between the two groups in Germany, with just **60% of ITDMs** expecting the number of attacks to increase



WILL THE SEVERITY OF CYBER ATTACKS INCREASE NEXT YEAR?

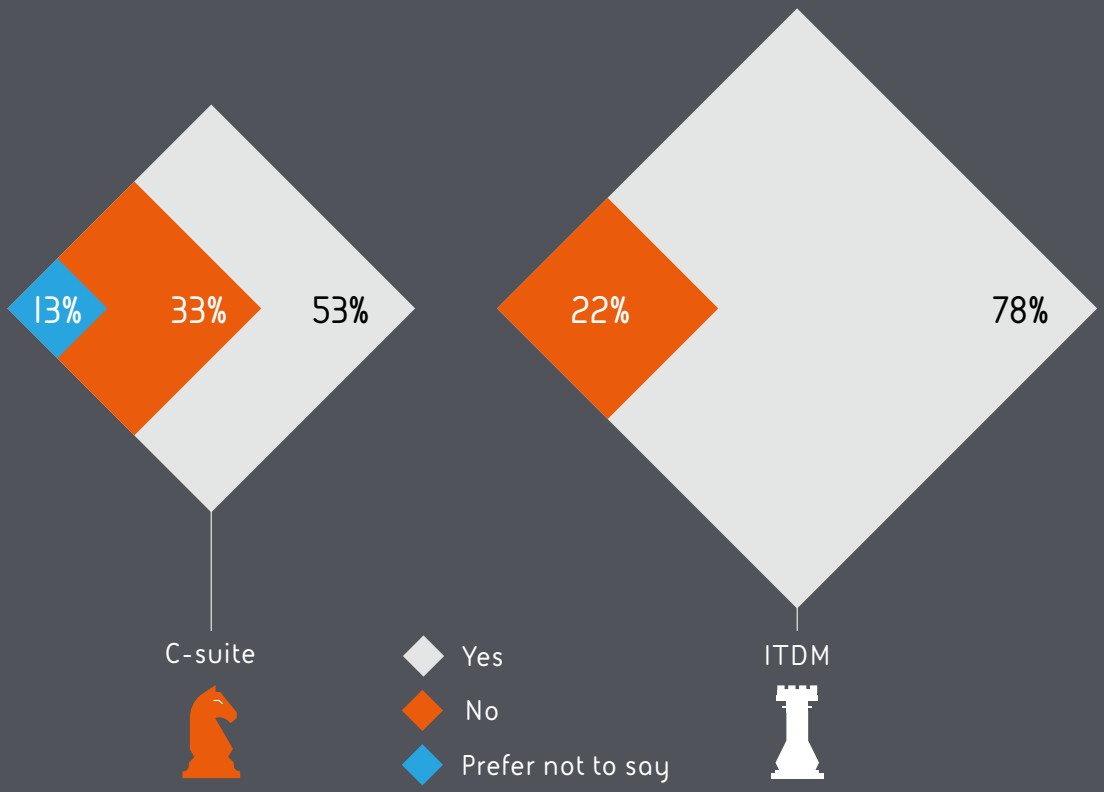
Australian C-suites are least likely to think attacks will increase in number (47%) whilst 90% of German C-suites believe they will.



CHAPTER 5

Strengthening defences from the inside out

Outsourcing may come with connotations of cost-cutting elsewhere, but in the world of cyber security, sharing the job of defence with specialists is business as usual for many of the people we spoke to. Economies of scale, specialist facilities, shared intelligence and the ability to call upon skills that are in high demand: all these things make some sort of outsourced defence attractive. And it's reflected in the numbers: nearly four out of five ITDMs (78%) say they call on third parties. The number for C-suite respondents is lower, but 13% of respondents were reluctant to say whether they outsource or not. Clearly, however, there's no shame in having domain experts on call: on average, between 27% and 28% of cyber security and defence capabilities are outsourced to another organisation.



OUTSOURCE SECURITY AND DEFENCE TO ANOTHER ORGANISATION

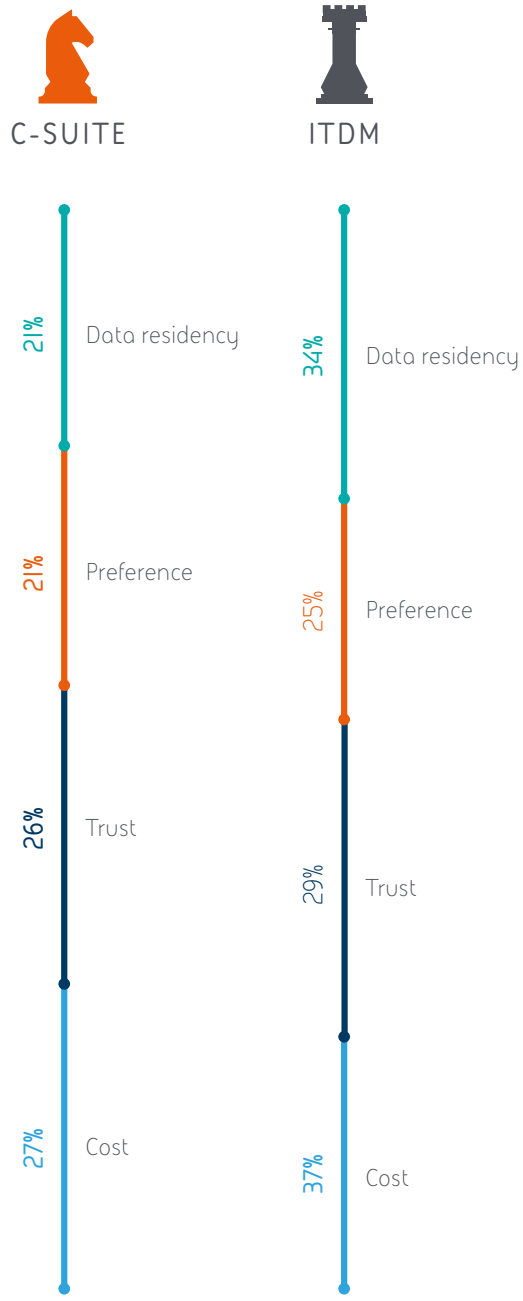
Between 27% and 28% of cyber security and defence capabilities are outsourced to another organisation

Why outsource?

It's a good question: given that most companies seem to be outsourcing and gaining significant benefit from doing so, why would organisations not want to pass more of the responsibility on to expert third parties? As with many things, it comes down to the law and money. For nearly four in 10 ITDMs the issue of cost represents a significant blocker to buying more outsourced or managed services. A second compelling reason for over a third of ITDMs is Data Residency - put simply, where in the world your organisation's data is stored.

Storing or processing your - or your customers' - data in another place can raise all kinds of regulatory problems, something that the C-suite is also aware of, since just over a fifth of C-suite respondents cited Data Residency as a barrier to outsourcing. However, executives are also concerned about cost (some 27% cited it), closely followed at a single percentage point lower by trust. A fifth simply prefer to have their cyber security skills and capabilities in-house.

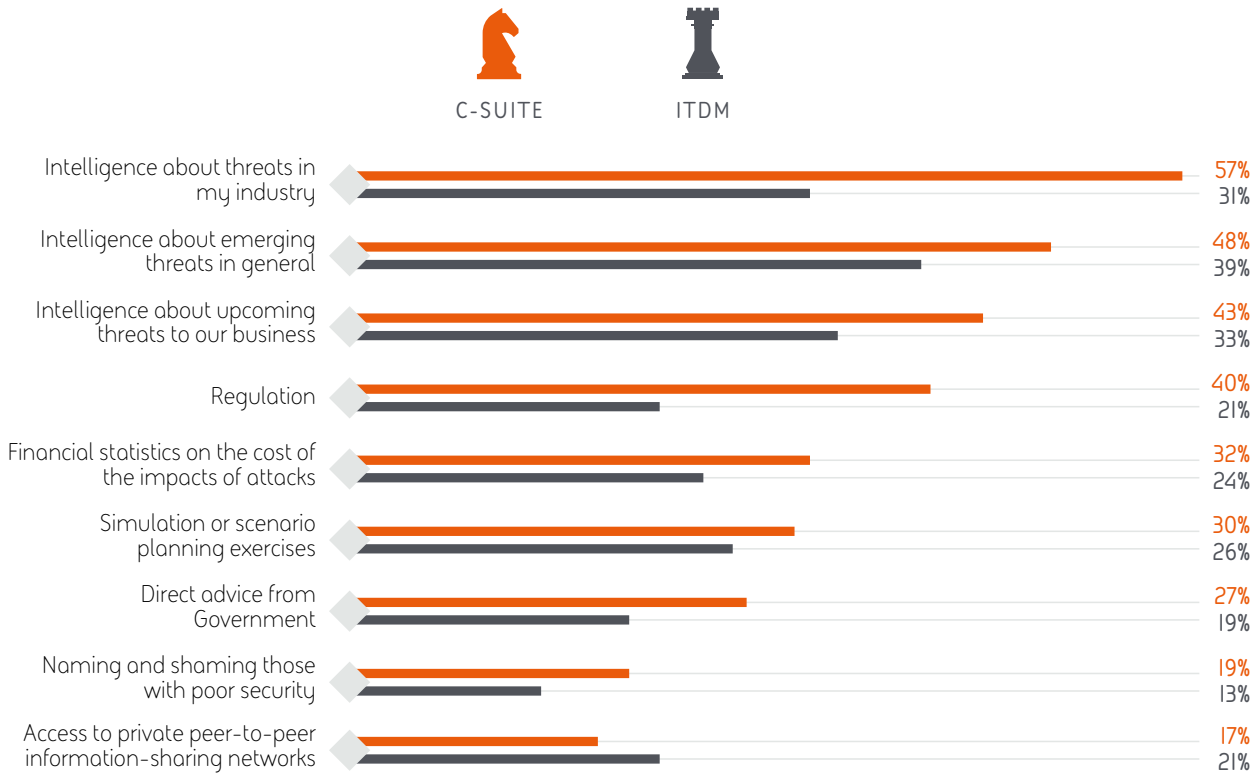
Outsourcing may come with connotations of cost-cutting elsewhere, but in the world of **cyber security,** sharing the job of **defence** with specialists is business as usual



BARRIERS TO OUTSOURCING MORE CYBER SECURITY AND DEFENCE CAPABILITIES

What should I outsource?

It's no surprise – one of the top things organisations wanted to rely on from outside was intelligence. Threat Intelligence, especially when combined with a comprehensive understanding of one's own weaknesses, allows an organisation to understand what adversaries it will most likely face, what they'll be looking for and their likely methods of attack. In turn, this gives organisations a chance to think strategically – and point more of their resources and defences towards the most likely avenues of attack. No wonder C-suite workers and ITDMs both agreed that intelligence about emerging threats, those within their sector and potential new threats came in over and above other ways of combatting cyber attacks. Perhaps surprisingly, C-suite respondents had more of a consensus on the value of great threat intel than ITDMs. They also seemed to be big fans of regulation.



MOST EFFECTIVE WAYS IN HELPING TO COMBAT POTENTIAL CYBER-ATTACKS

Perhaps surprisingly, business leaders had more of a consensus on the value of great threat intel than ITDMs. And, unusually, they also seemed to be big fans of regulation

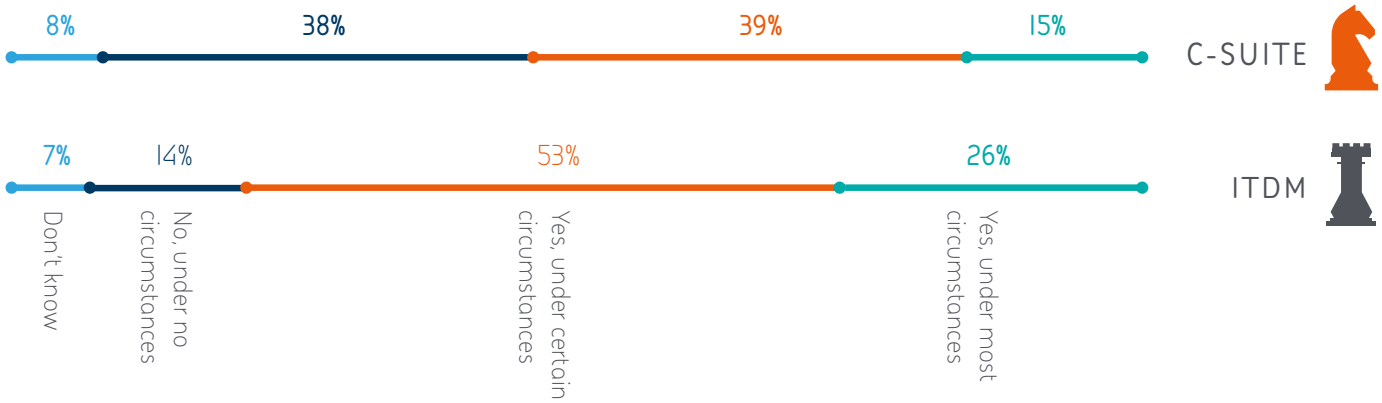
Naming and shaming – not so hot

There was low support for the idea of naming and shaming organisations that fell below the required standards of protecting their networks and customers. This is hardly surprising, as it's likely to attract further attacks, and even if it does spur a business on to protect itself more thoroughly, the likely damage to its reputation will outlast the original reason for disclosure. It's not surprising that robust regulation is viewed by twice as many C-suite respondents and nearly double the amount of ITDMs as a more effective method of addressing the problem.

Data sharing – a mixed bag

Both groups proved willing to pool data with other organisations, if it would make it easier to spot irregular activity. We posed this question for a very simple reason: The more data on potential attacks is collected together, the easier it can be to pull certain patterns of behaviour out. What might seem random or irrelevant traffic to a single organisation can build up into a more worrying story when viewed amongst peers from a suitable distance.

Our respondents were generally in favour of the idea – 54% of C-suite respondents were open to data sharing under most or certain circumstances, and the number rose to 79% amongst ITDMs. Yet, there was also considerable suspicion: 38% of C-suite respondents, or nearly two in five – would not be willing to share under any circumstances. With the concerns expressed elsewhere in the survey around competitors as a source of attacks, this is, perhaps, understandable.



ORGANISATIONS WILLING TO SHARE DATA TO MAKE IT EASIER TO SPOT ILLEGAL ACTIVITY

So what?

Outsourcing isn't an option, it's an imperative. Outsourcing some of their cyber security allows organisations, however large, to pool resources in a way that's effective and saves money. This is particularly important when it comes to Threat Intelligence. Sharpening up one's cyber security these days means buying in the right services for the right job – and keeping a strong review process going to make sure those services remain effective.

Conclusion

One thing is clear from the responses we received: there is no magic technological bullet. The biggest positive change any organisation can make, it seems, is not necessarily to buy the latest and greatest security product, but to improve its own internal communications. Our research demonstrates that those charged with business risk, and those responsible for IT, have the same intentions, goals and aspirations for their organisations. The catch is this: they don't perceive the threat, the treatments or the solution in the same way.

Outsourcing some security functions, building (and agreeing upon) shared strategic plans that lay out both strategic and ad-hoc spend, and understanding the potential impact of identifying, halting and repairing a breach are all solid steps towards sharpening one's cyber security stance. They are, however, built on a common foundation: improving communications. Without a common understanding of the desired destination, and the means by which they'll reach it, IT Decision Makers and C-suite executives risk all.

Those charged with business risk and those responsible for IT have the same intentions

The catch is this: they don't perceive the threat, the treatments or the solution in the same way

Cyber risk – and associated worries – have reached the top of the agenda for many boards of directors over the last few years, and quite rightly so. Cyber security is now a business risk issue like any other. But how different groups within your company perceive this risk is another thing. Whether you're an IT director or a C-level executive, one thing is clear: you need to do more than talk to each other: you must make yourselves understood.

Methodology

Opinium conducted a global survey of business leaders and IT Decision Makers in Australia, Canada, Germany, Malaysia, Singapore, United Arab Emirates, the UK and the US.

Between 17 October and 21 November 2016, 221 telephone interviews were conducted with C-suite representatives (CEOs, CFOs, COOs, CIOs and CTOs) of Fortune 500 businesses, and 984 online interviews were conducted with IT Decision Makers involved in IT security in businesses with more than 50 employees.

About Opinium

Opinium is an award-winning strategic insight agency built on the belief that in a world of uncertainty and complexity, success depends on the ability to stay on the pulse of what people think, feel and do. Creative and inquisitive, we are passionate about empowering our clients with the data to make the decisions that matter. We work with organisations to define and overcome strategic challenges – helping them to get to grips with the world in which they operate. We use the right approach and methodology to deliver robust insights, strategic counsel and targeted recommendations that generate change and positive outcomes.

www.opinium.co.uk

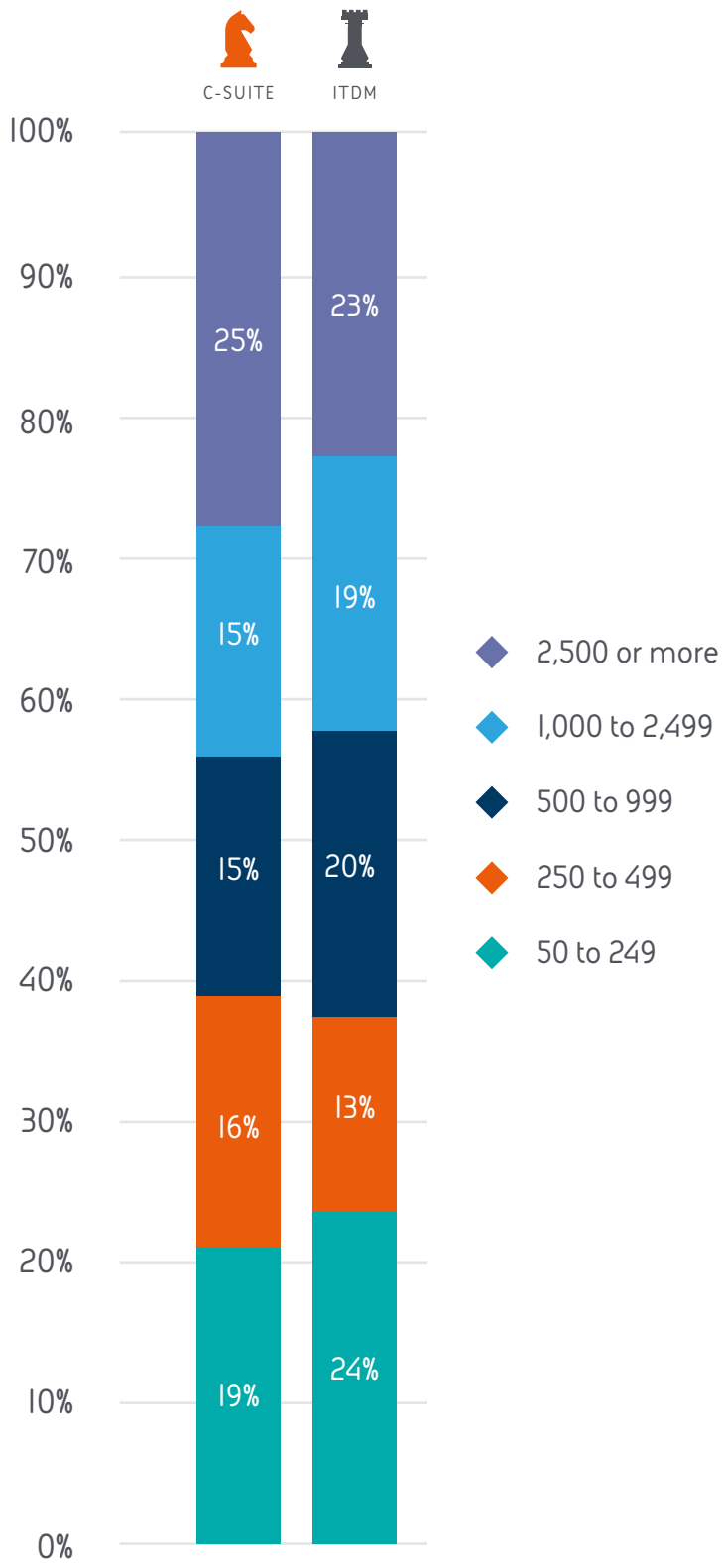
research@opinium.co.uk

0207 566 3190

Appendix A

Company sizing by employee numbers

Differences between C-suite and ITDMs respondents are probably partly driven by company size, but overall they compare fairly equally



Country view:
United Arab Emirates

ITDMs in the United Arab Emirates market appear far less worried at the prospect of a cyber attack than their counterparts around the world. In fact, the number who said they were concerned about cyber security is lower than in any other market we surveyed. Less than a third (31%) said the most significant challenge facing their business was cyber security, compared with over half in Australia (52%), Singapore (53%) and Canada (52%).

The number of ITDMs in the UAE who thought it likely their business would be targeted by a cyber attack in the next 12 months was also lower than in any other market, at 62%, compared with more than three quarters (79%) in the UK and 80% in Malaysia.

It may be that companies in the region have invested significantly in technology to detect and prevent attacks, which has served to allay many of their fears. Little regulation in this area may also give ITDMs less pause for thought in their day-to-day working lives when it comes to potential threats. Another possible reason is that awareness of cyber attacks outside of their business is low, as these are not typically reported in the local press.

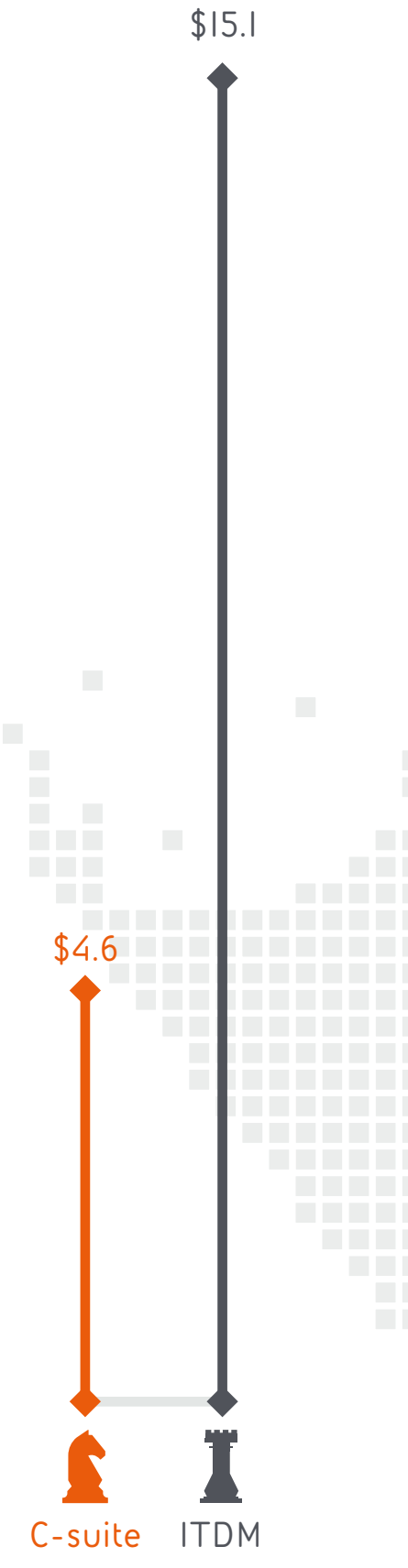
> Where the C-suite and ITDMs in the UAE **both agree** is that they are seeing the level of alerts increase

This could also account for the discrepancy in response from the C-suite, who have more of a global market view. A much higher number – 67% – say that cyber security is their greatest concern.

Where the C-suite and ITDMs in the UAE both agree is that they are seeing the level of alerts increase. Sixty-three per cent of C-suite respondents and almost half of ITDMs (47%) agree on this, a higher percentage than in any other market.

This is no doubt due to the increasing number of cyber threats businesses are seeing across the globe, but may also be the result of more sophisticated technology picking up a higher number of potential threats, as well as a lack of the right knowledge and skills to eliminate false positives.

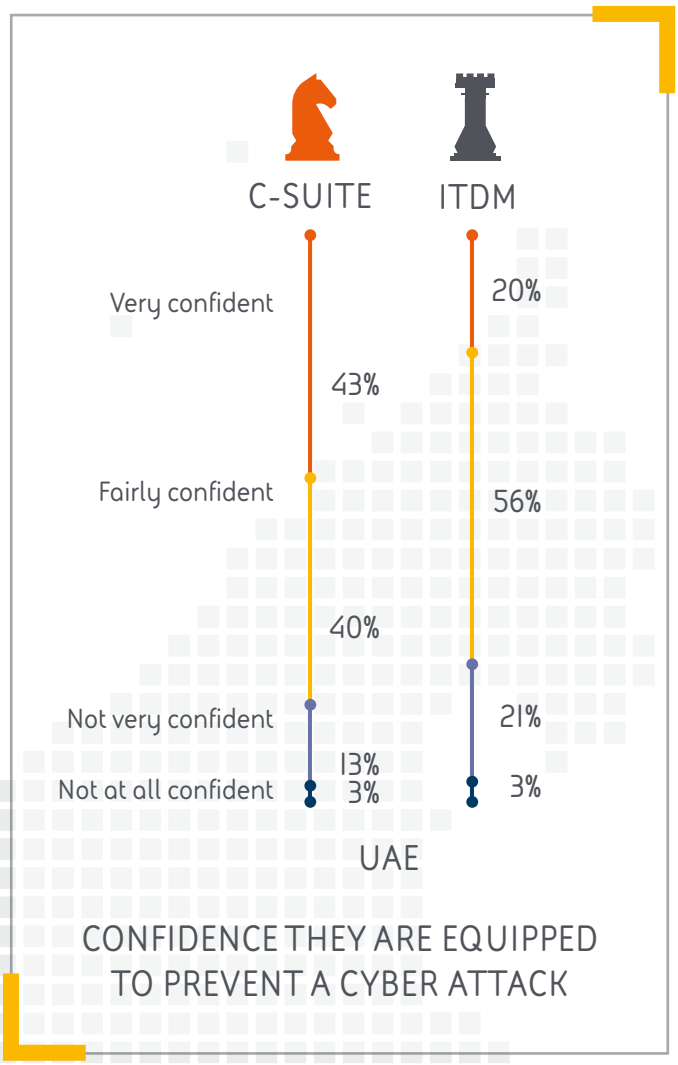
Even though 70% of C-suite respondents in the UAE market expect the number of attacks to increase, conversely only 40% of them say they are likely to increase their allocation of time and resources on cyber security and defence in the coming year, the lowest percentage of any market. This points to a perception among businesses that they are more secure than they might actually be.



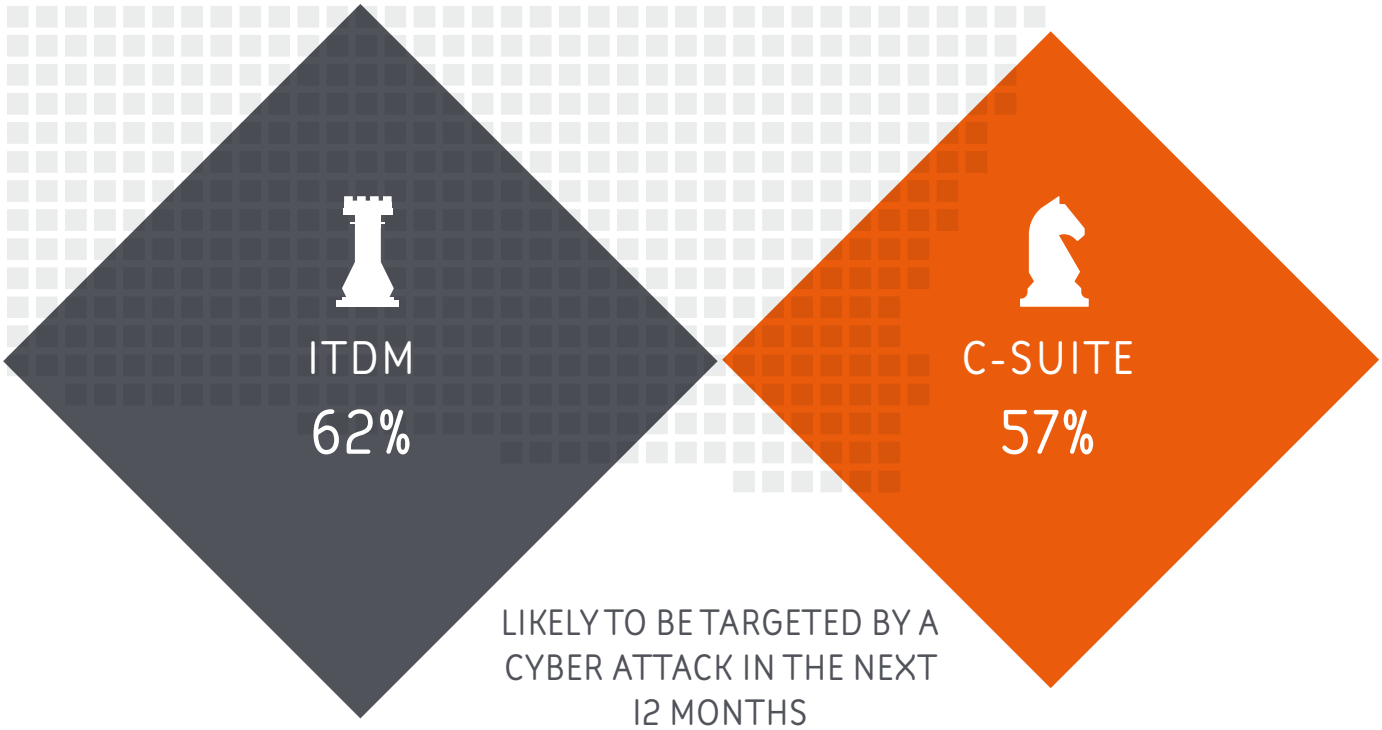
COST OF AN ATTACK IN US$. AVERAGE (MILLIONS)

67% of business leaders say that cyber security is their greatest concern

47% of ITDMs say they are seeing the level of alerts increasing



CONFIDENCE THEY ARE EQUIPPED TO PREVENT A CYBER ATTACK



LIKELY TO BE TARGETED BY A CYBER ATTACK IN THE NEXT 12 MONTHS

Country view: Malaysia

Malaysians are extremely wary of the growing cyber threat, with the vast majority of ITDMs (80%) believing they will be targeted by a cyber attack in the next 12 months – the highest percentage of any market surveyed.

Their fears appear to be justified; Malaysia Computer Emergency Response Team (MyCERT) statistics show that last year alone, over 2.7 million botnet drones and malware infection attacks were reported in the country, plus over 9,000 cyber security incidents.

Both C-suite respondents and ITDMs are concerned about the growing threat, with 90% of C-suite and 84% of ITDM respondents believing the number of attacks will increase in the next year, and similar numbers (90% and 87% respectively) believing attacks will be more severe.

What's more, almost a third (30%) of Malaysian C-suite respondents, a larger proportion than in any other market, are not sure they are equipped to handle a cyber attack, should they be targeted; both ITDMs (2%) and the C-suite (0%) lack confidence that they have the right skills in house.

84% of ITDMs think they have the right controls in place

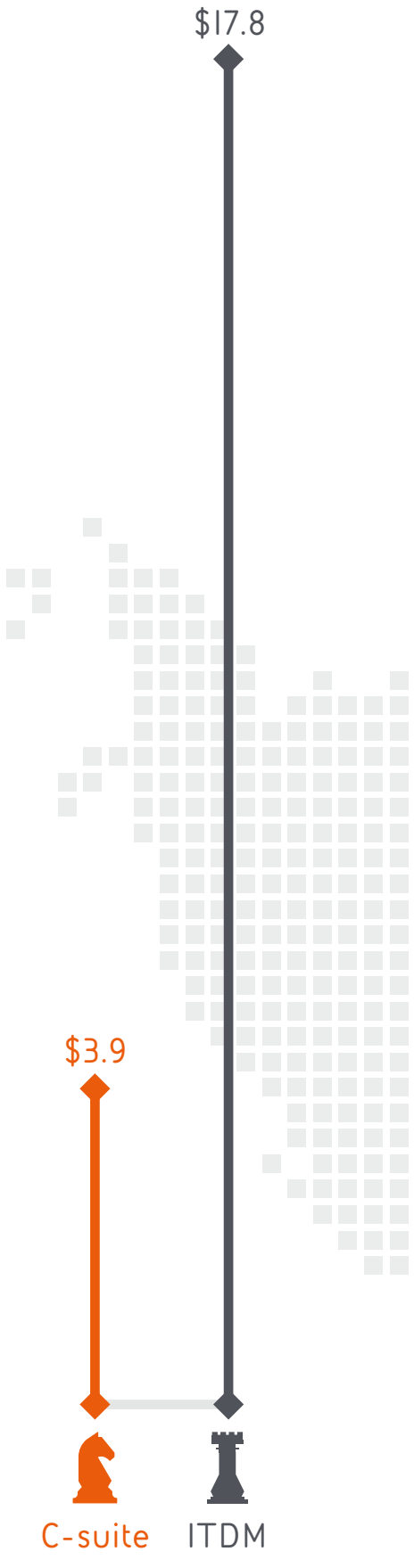
In a bid to combat this and support businesses, The Securities Commission (SC) in Malaysia recently issued 'Guidelines on Management of Cyber Risk', which focuses on improving cyber resiliency for all market participants.

Both ITDMs (35%) and C-suite respondents (55%) in Malaysia agree that intelligence is the most effective tool in helping businesses deal with potential attacks, and the government appears committed to making cyber security a priority. In his keynote address at Singapore International Cyber Week (SICW) 2016, Malaysia's Science, Technology and Innovation Minister said there was a need to develop a national cyber security innovation ecosystem.

When it comes to the nature of the threat, 70% of Malaysian C-suite respondents think an attack is most likely to come from hobbyist hackers, but insider attacks from suppliers also present a significant worry.

C-suite respondents' knowledge of current cyber-defences appears to be low, with only 15% of those surveyed saying they have a dedicated Security Operation Centre (SOC), compared to almost a third of ITDMs (32%). There is also a disconnect when it comes to confidence in security controls for cloud services. Eighty-four per cent of ITDMs think they have the right controls in place, compared to only 35% of C-suite respondents.

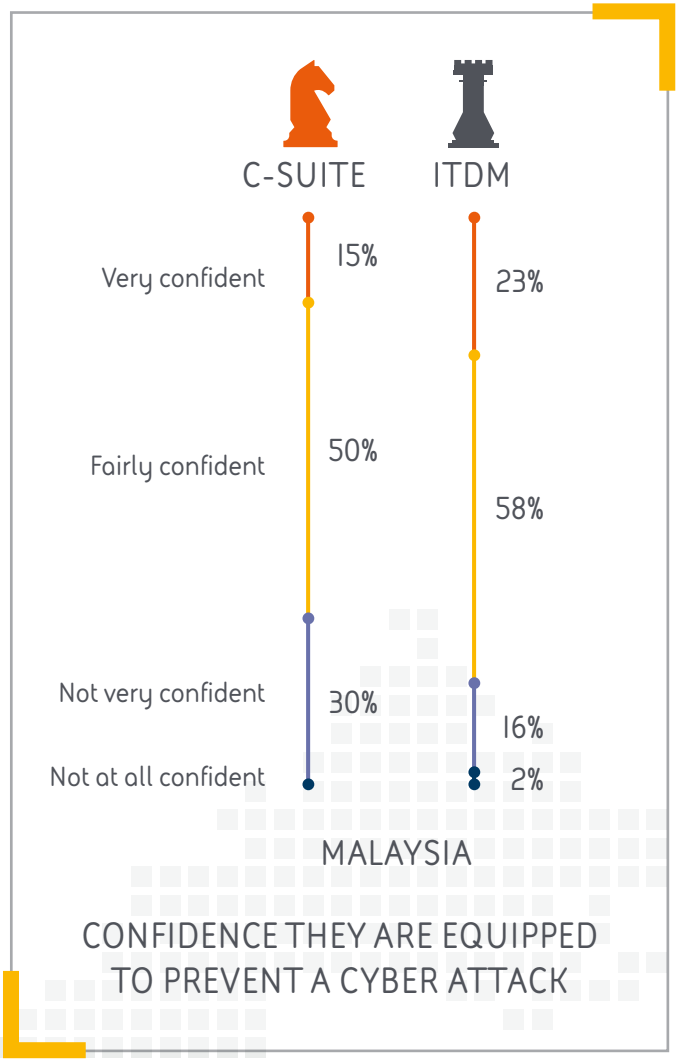
Seventy per cent of Malaysian executives believe underfunding of IT security might be a reason for a successful attack, yet it's within their power to remedy this and improve their defences.

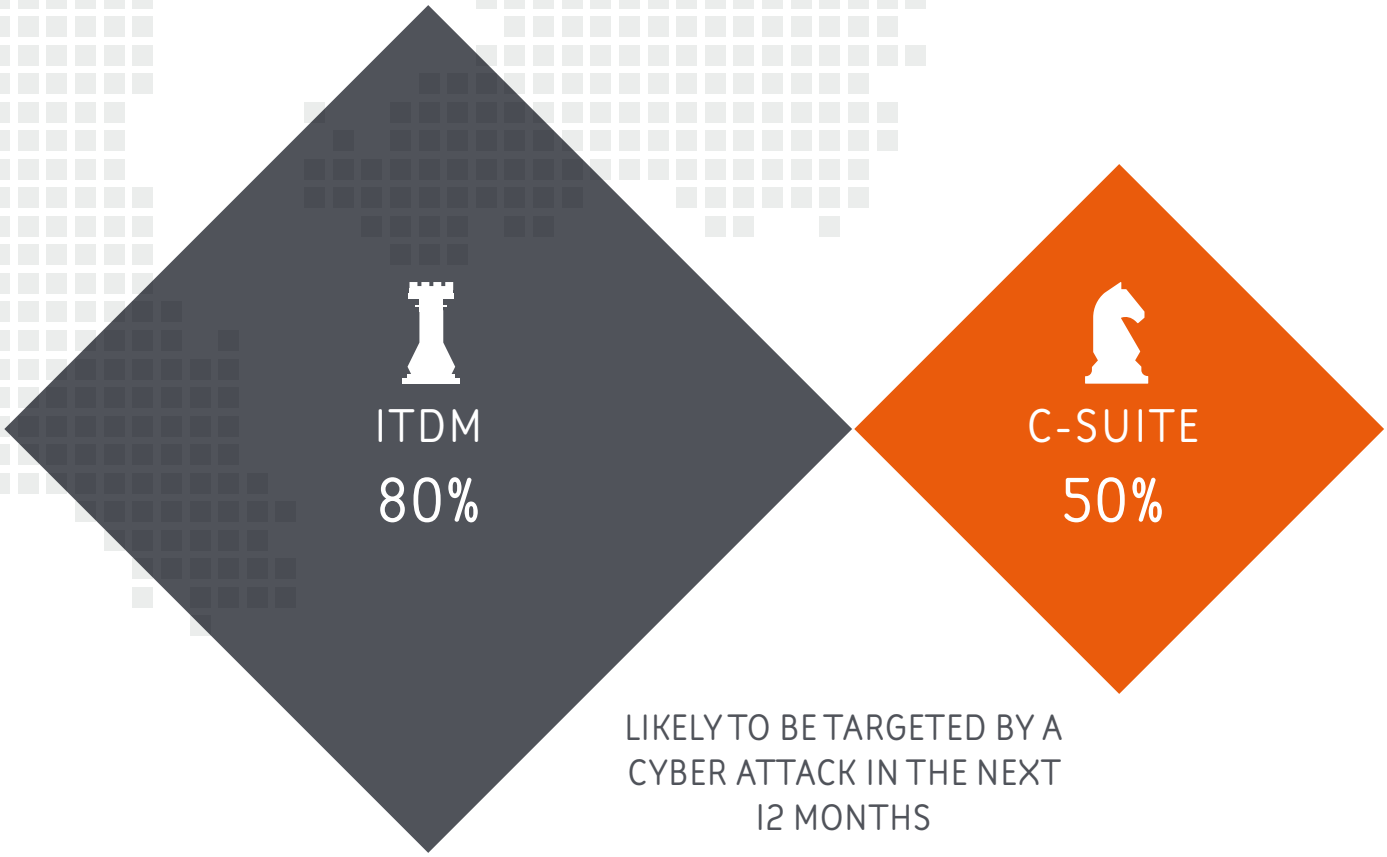


COST OF AN ATTACK IN US$. AVERAGE (MILLIONS)

90% of C-suite believe the number of attacks will increase next year

Only 2% of **ITDMs** belive they have the right skills in house





Country view: Singapore

C-suite respondents and ITDMs in Singapore appear at odds when it comes to the issue of cyber security, both in terms of the nature of the threat and their defence strategy.

More than three quarters (76%) of C-suite respondents think cyber security is the biggest challenge facing their business, as do just over half of ITDMs (53%). However, significantly more ITDMs than C-suites think their business will be targeted by a cyber attack in the next year (77% and 48% respectively). C-suite respondents and ITDMs in Singapore don't align on who presents the greatest risk either. Only 38% of business leaders view professional hackers as the biggest threat to their business, compared to 60% of ITDMs.

As Internet usage increases in Singapore, the government is stepping up its efforts to protect businesses and individuals from cybercrime. In 2016, Singapore's Cybersecurity Strategy was announced, with the aim of creating a resilient and trusted cyber environment. To effectively deal with the threat of cybercrime, the government is also implementing a National Cybercrime Action Plan.

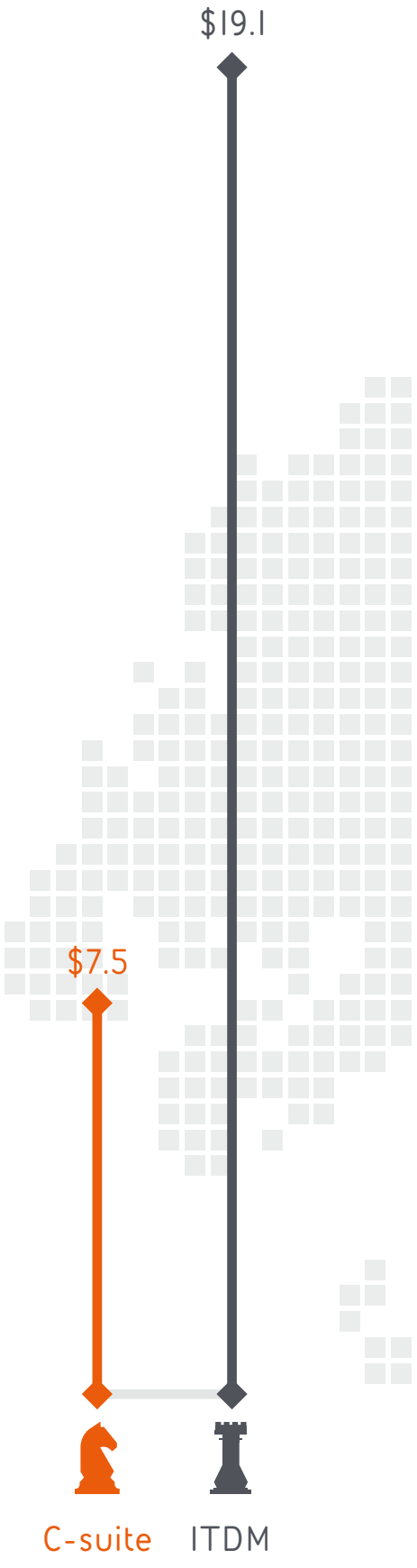
A significant proportion of Singaporean C-suite respondents lack confidence in their ability to handle a cyber attack; 14%, the largest proportion of C-suite respondents in any market, say they are not at all confident in the event of an attack occurring. This compares to a global average of 3%. What's more, only 11% of ITDMs in Singapore say they are very confident in their ability to handle a cyber attack, which compares to 20% globally.

Only 11% of ITDMs say they are very confident in their ability to handle a cyber attack

Trust in employees also appears to be low among C-suites. More than twice as many C-suite respondents (62%) think human error will enable a cyber attack than ITDMs (30%), who thought it would most likely be attackers breaching their network.

Despite this lack of confidence in employees, Singaporean C-suite executives appear keen to lay responsibility for cyber security at the feet of anyone but senior leadership, with 66% saying it's the responsibility of either the IT team or all staff. Singaporean ITDMs, however, aren't of the same view, with 51% saying it's the responsibility of senior management, including the CEO.

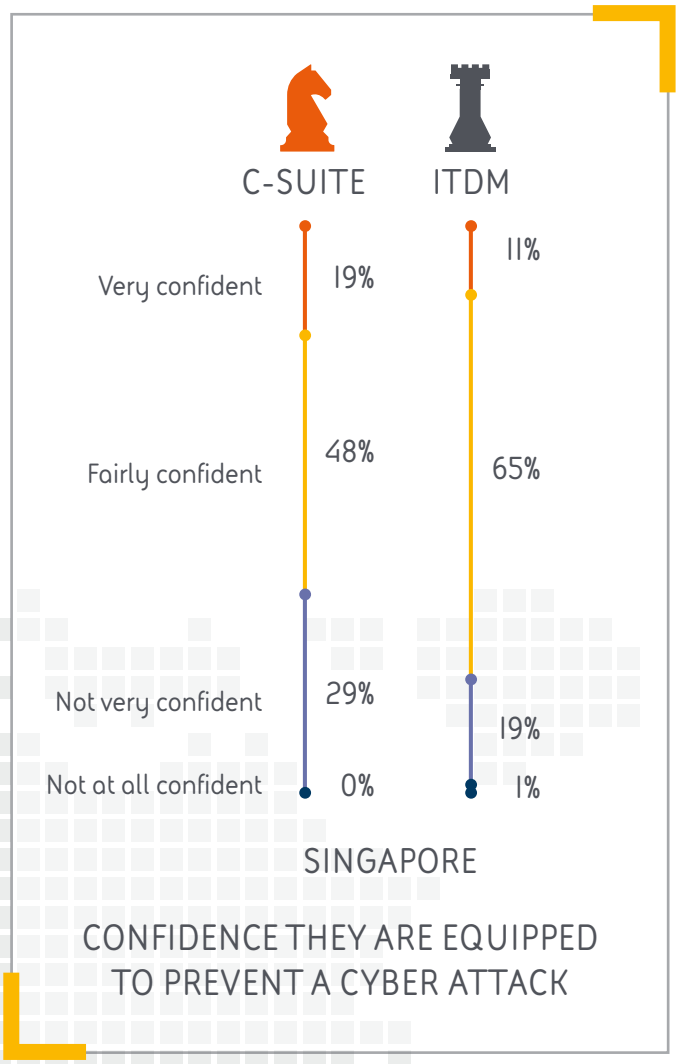
The one thing that ITDMs (81%) and C-suite (80%) respondents in Singapore do agree on is their belief that the number of attacks will increase in the next year. C-suites in Singapore also report seeing more alerts. Sixty-two per cent say the level of alerts are increasing. However, with only 28% of ITDMs saying the same, it could just be that C-suites are being kept better informed than they have been previously.

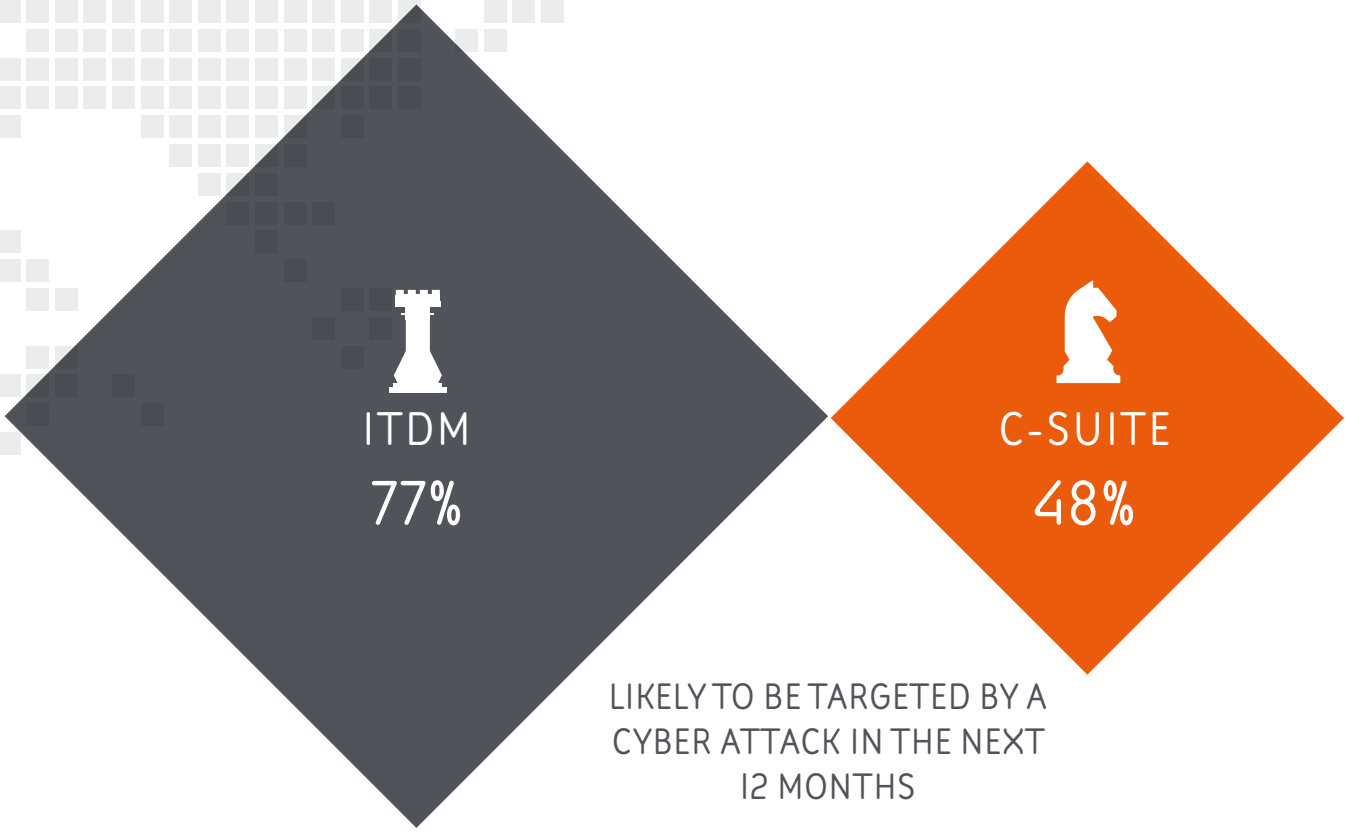


COST OF AN ATTACK IN US$. AVERAGE (MILLIONS)

76% of executives think cyber security is the biggest challenge they face

51% of ITDMs believe senior management is responsible for cyber attacks





Country view: Australia

Australian C-suite respondents are far more wary of being hacked than their contemporaries. Seventy-three per cent of those surveyed think they are likely to be the target of a cyber attack, as do 77% of ITDMs, compared to 57% of those globally. Australian executives, aware of a series of high profile hacks, may feel a serious attack on their organisation is only a matter of time.

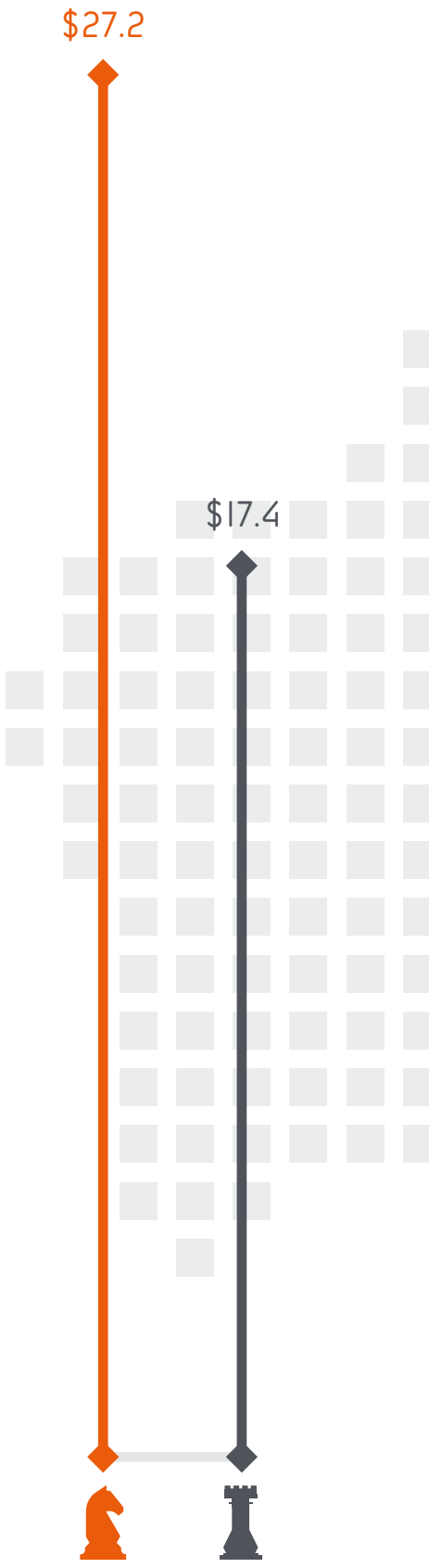
Being so aware of the consequences of a hack, both financial and reputational, may be the reason that Australia is the only market where C-suites estimate the cost of a serious, successful cyber attack to be higher than ITDMs – at US $27.2 million. Both the C-suite (83%) and ITDMs (47%) also rate professionals as far greater a threat than any other type of hacker, which may also contribute to their fear of a successful attack.

Cyber security is a priority for the Australian government, which released its Cyber Security Policy in April last year. This was followed by some key appointments including Australia's first Minister Assisting the Prime Minister on Cyber Security, and a special adviser to the Prime Minister on cyber security.

Half of C-suite respondents and ITDMs (50%) say they will increase the time and resources spent on cyber security and defence in the coming year. However, almost a quarter (23%) of C-suite respondents think they have all the necessary skills to deal with a cyber attack, while only 7% of ITDMs agree. Businesses are also being warned not to have a set and forget mindset when it comes to their cyber security strategy.

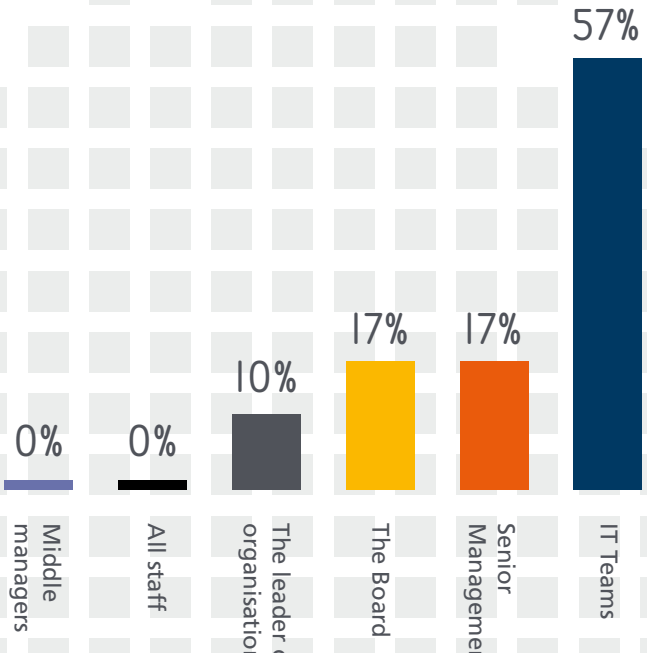
50% of C-suite respondents say they will increase resources spent on cyber defence

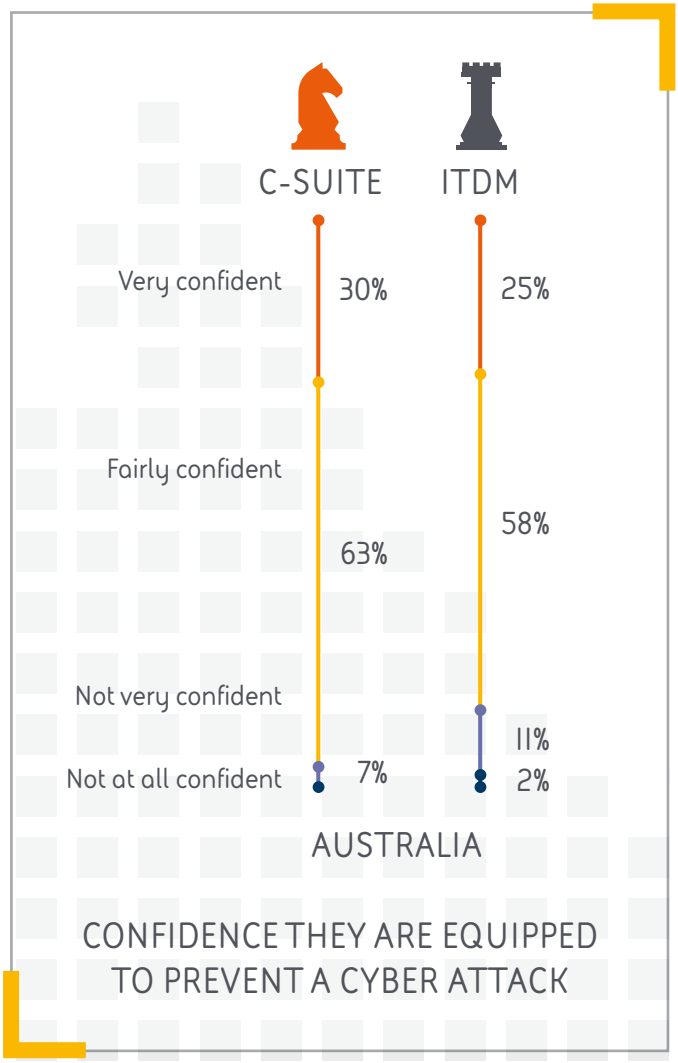
77% of ITDMs feel they are likely to be targeted by a cyber attack



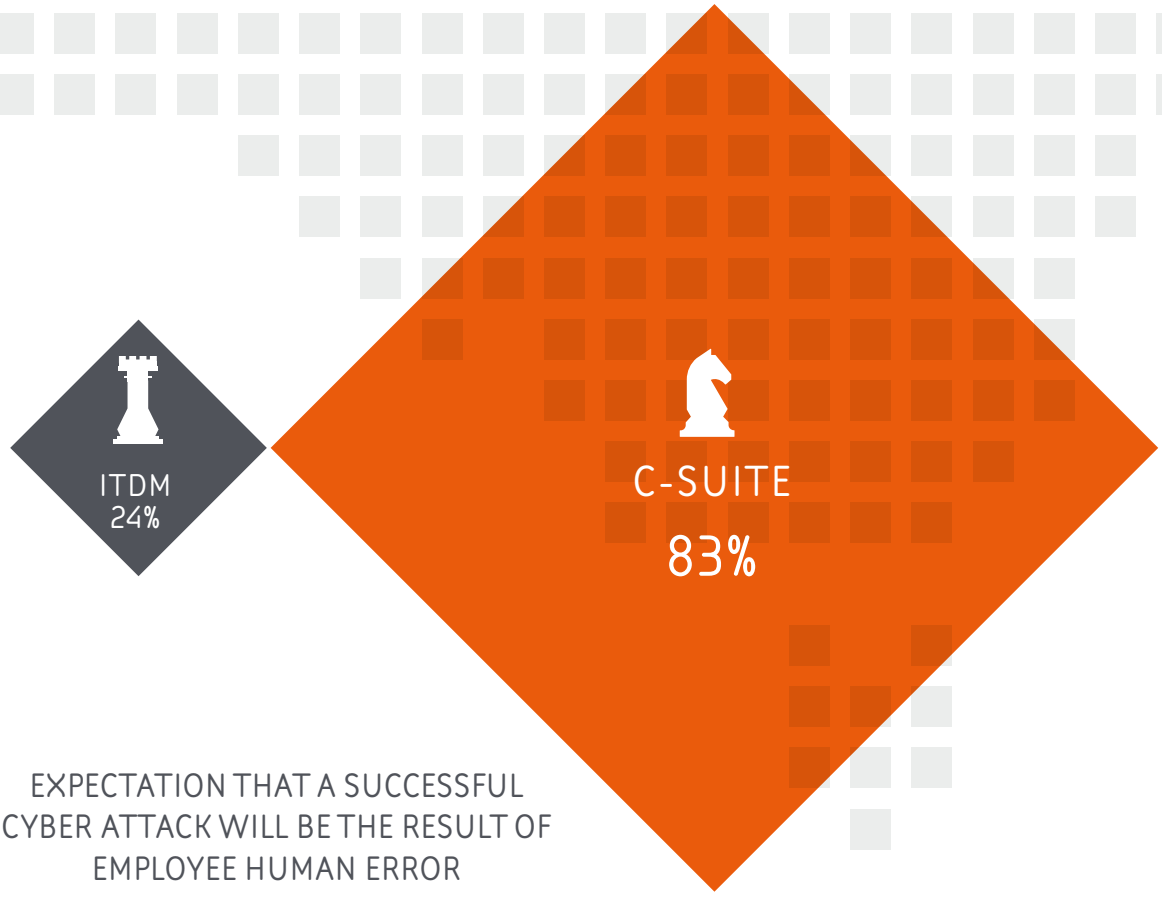
COST OF AN ATTACK IN US$. AVERAGE (MILLIONS)

57% of Australian C-suites believe the IT Team are responsible for breaches





CONFIDENCE THEY ARE EQUIPPED TO PREVENT A CYBER ATTACK



EXPECTATION THAT A SUCCESSFUL CYBER ATTACK WILL BE THE RESULT OF EMPLOYEE HUMAN ERROR

Country view: Germany

Of all of the countries surveyed in this year's Cyber Defence Monitor, Germany stands out as having some of the most divergent attitudes and approaches to cyber security, both against peers and between German C-suite and ITDM respondents.

There's a great deal of confidence from C-suite respondents – and compared to their peers in other countries, it's a striking figure. Fifty-nine per cent of C-suite executives in Germany see the increasing level of alerts compared to just 32% of ITDMs. Nine in ten C-suite respondents in Germany expected the volume of attacks to increase, while only 60% of their ITDM counterparts agreed.

When asked how likely they thought it that their business would be targeted for a cyber attack in the next 12 months, nearly a third (32%) of ITDMs in German organisations felt confident they would not be attacked. This is low when compared to counterparts in the UK (79%) and Malaysia (80%).

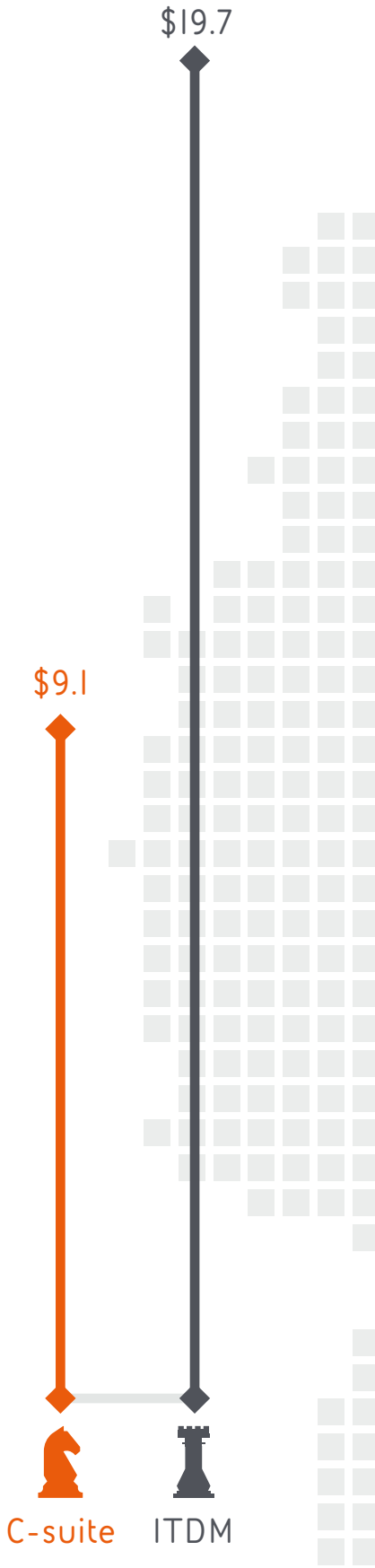
Two in five (40%) of German C-suite respondents expected an attack – compared to the global average of 57%. Half of German C-suite respondents felt that attackers would be most likely to be competing businesses; only 24% of C-suites worldwide picked competitors as a threat.

Perhaps the biggest difference in perceptions within German organisations is that of cloud adoption. Three in five (60%) C-suite executives say their organisation does not use cloud services – yet only 16% of German IT Decision Makers agreed with them.

One potential reason for the C-suite saying their businesses do not use cloud services could be that they have concerns about the implications of storing data in the cloud. Only 37% of German business leaders expressed confidence that their organisation had the right cloud security controls in place - a figure only matched by business leaders in Singapore at 33% and Malaysia at 35%.

That said, German respondents were unanimously confident in the resilience of their security governance and IT security software – although mobile device usage and home working were not so confidence-inspiring.

Only 37% of C-suite respondents had confidence they had the right cloud security in place



COST OF AN ATTACK IN US$. AVERAGE (MILLIONS)

German ITDMs are some of the most confident on tackling cyber crime

75%

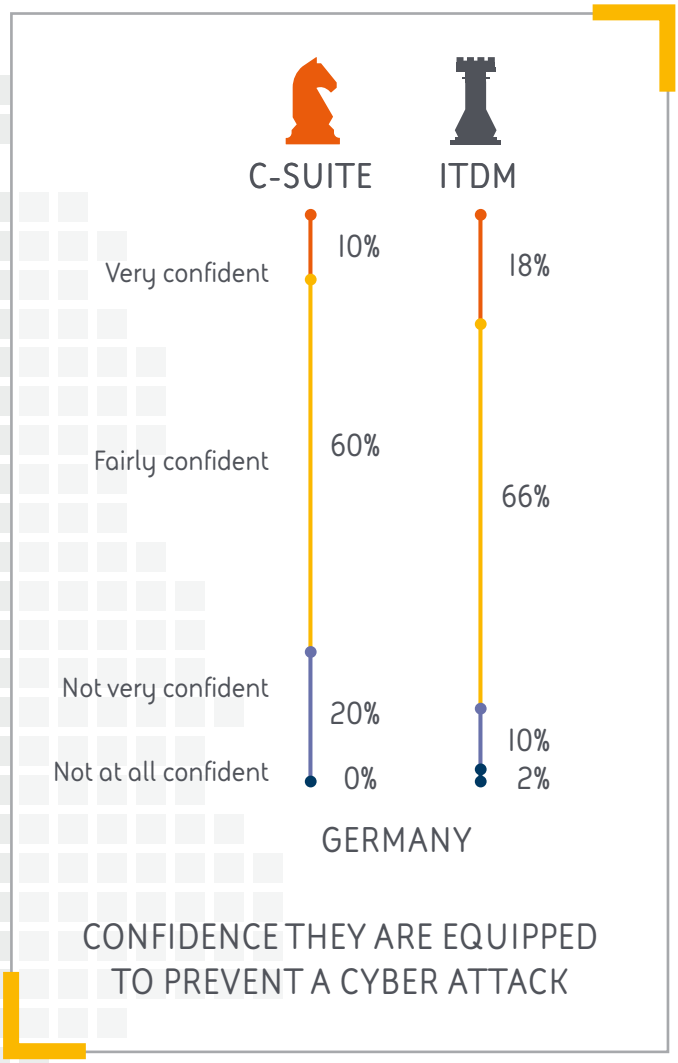
We have enough support from suppliers, enforcement agencies and government to tackle cyber security

82%

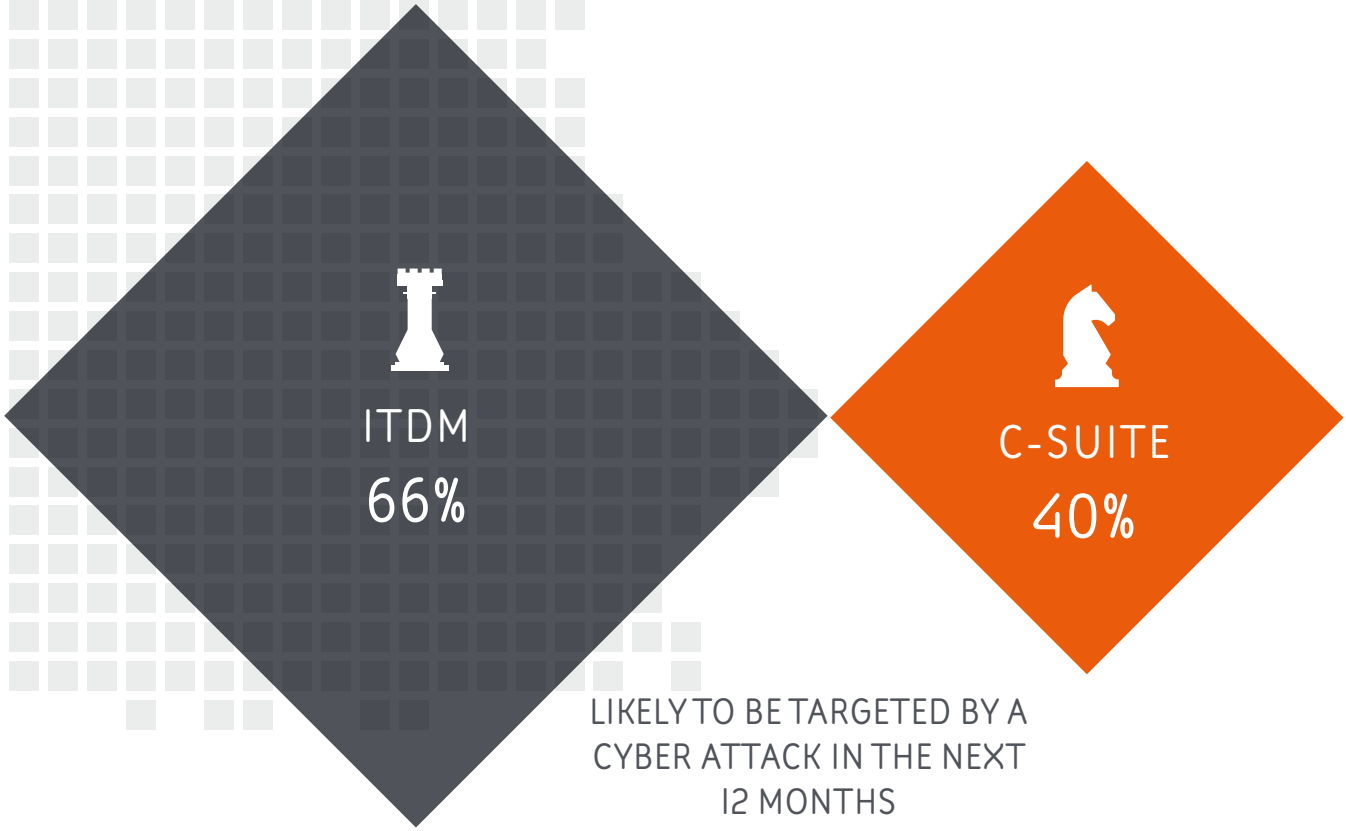
We have enough information to make informed decisions on cyber security

81%

Our board takes the risk of cyber attack seriously



CONFIDENCE THEY ARE EQUIPPED TO PREVENT A CYBER ATTACK



LIKELY TO BE TARGETED BY A CYBER ATTACK IN THE NEXT 12 MONTHS

Country view: United Kingdom

C-suite respondents in the UK think they spend less of their IT budget on cyber security than their peers – 7% of budget, compared to 10% worldwide – the lowest figure of any national grouping of C-suite executives.

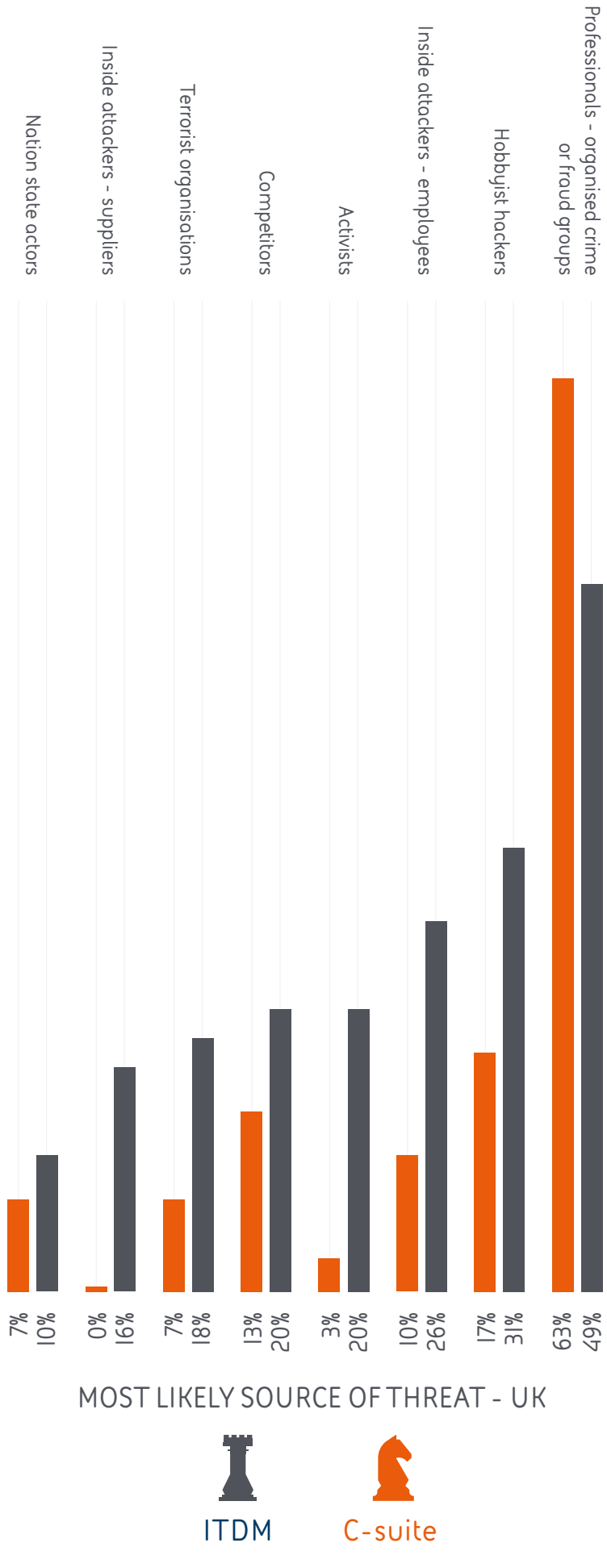
ITDMs in the UK are enthusiastic about the cloud, mirroring general C-suite enthusiasm for the idea; 37% of the ITDMs surveyed in the UK predicted they would increase spending on cloud services.

There was also a significant focus on organised attack groups amongst both ITDMs and executives in the UK. Professionals – organised crime or fraud groups – were regarded as the most likely threat actors, while ITDMs also picked hobbyist hackers as the second most likely attack source.

This is matched by recent findings from the UK's Office for National Statistics, which for the first time earlier this year included computer misuse in its annual Crime Survey for England and Wales. The survey recorded 5.6 million incidents involving fraud and computer misuse, and while the overall trend in crime in the UK shows a decline in reported offences from 1995 onwards, these statistics only incorporate cyber-related crimes for the first time this year.

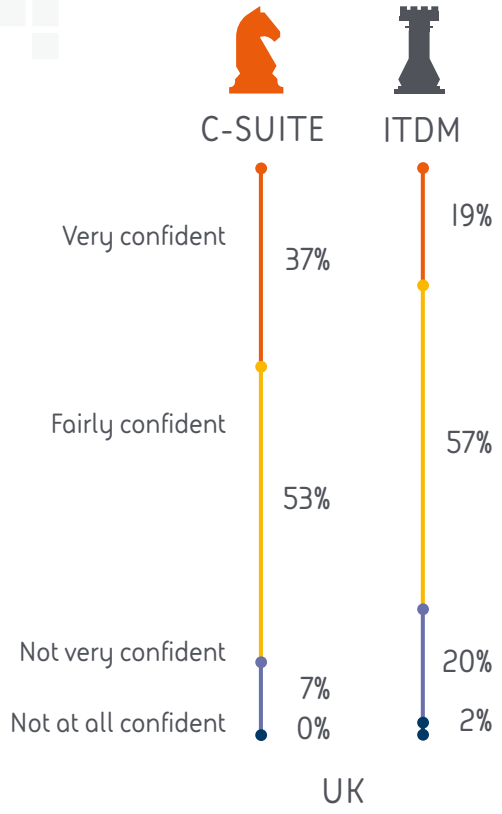
UK ITDMs also point to some interesting reasons why an attack on their organisation might succeed. A breach from outside is the most likely reason – but ITDMs also cite insufficient investments in IT security (34%) supply chain vulnerabilities, outdated software and deliberate security breaches by an employee.

Another area of interest in the UK: the business leaders we spoke to argued almost overwhelmingly that the IT team in their organisation holds the ultimate responsibility for security breaches, with 47% holding their IT department accountable. In contrast, ITDMs believe their organisation's leader, senior management and the Board are responsible. The figures reveal a significant difference of opinion between these two groups, and likely some interesting future discussions about responsibility and accountability in the event of a successful attack.

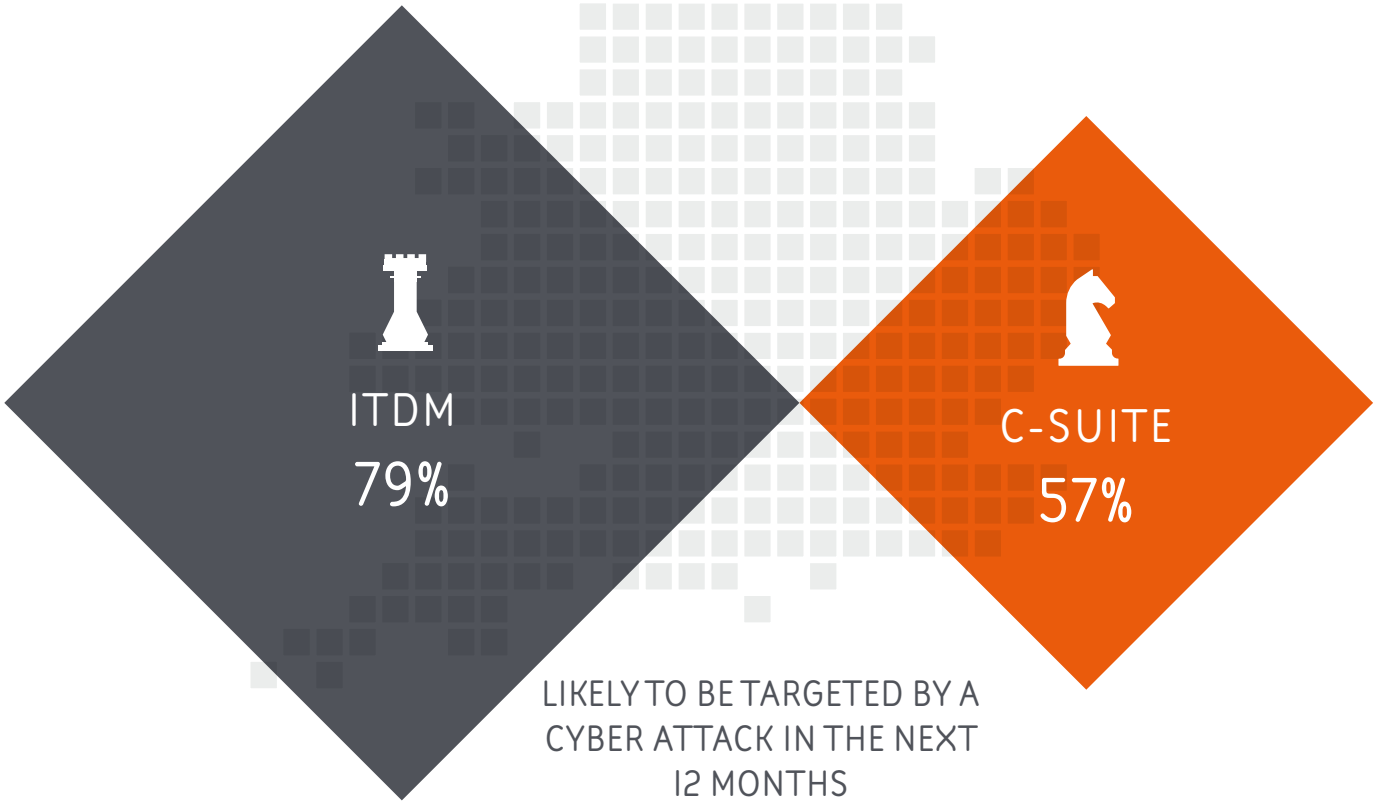


47% of C-suite respondents hold their IT department accountable for a breach

34% of ITDMs believe there is insufficient investment in IT security



CONFIDENCE THEY ARE EQUIPPED TO PREVENT A CYBER ATTACK



LIKELY TO BE TARGETED BY A CYBER ATTACK IN THE NEXT 12 MONTHS

Country view:
United States of America

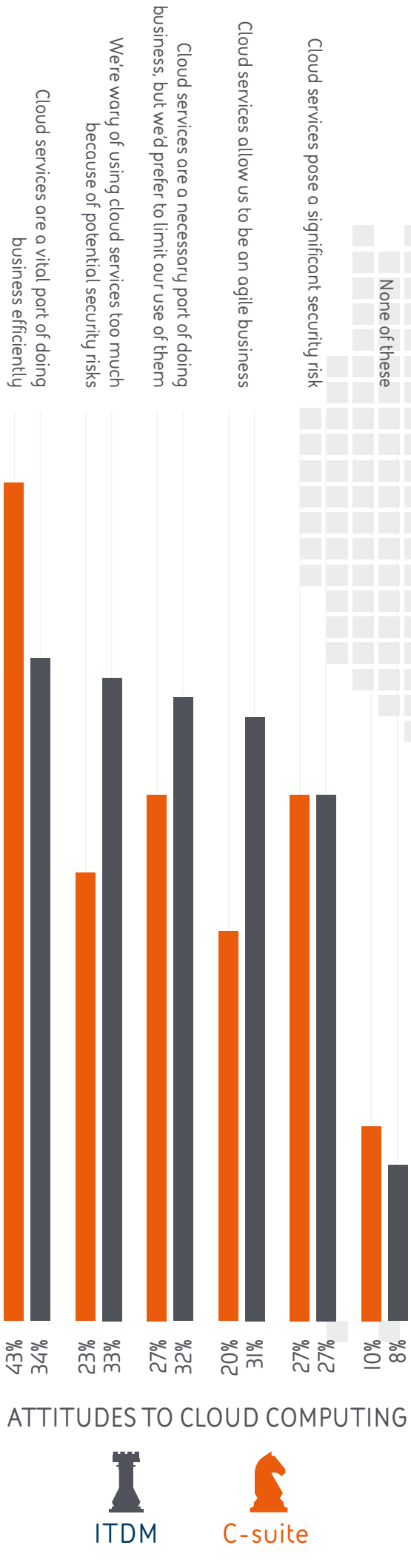
US respondents to our survey were confident in the ability of their business to fend off a cyber attack. As with C-suite respondents in the UK, US business leaders indicated that 7% of their organisation's IT budget was spent on cyber security and defence, lower than the worldwide figure of around 10%.

The results show a significant difference in how the two types of respondent (ITDM and C-suite) viewed the threat landscape. While both groups viewed organised crime as the most likely source of attack, nearly a third (32%) of ITDMs saw terrorist organisations as a likely source of attack – compared to just 7% of C-suite respondents, who were more likely to suspect professional crime groups.

IT Decision Makers in the USA responded far more actively to the question of where and why they would invest extra resources in cyber security, with over half (56%) wanting to minimise their security risk, something that was a reason for only 22% of C-suite respondents. American C-suite respondents were most concerned with keeping up to date with current and new threats and minimising risk. Reassuring customers came low on the list at 6% (compared to 27% of ITDMs), in line with the need to respond to a successful attack on the business.

When it came to cloud computing, the two groups formed something of a consensus around cloud security concerns. Almost a third (27%) of both groups saw cloud services as posing a significant security risk, although 31% of ITDMs also saw the services as supporting more agile business practices. Both groups (27% of C-suite respondents, 32% of ITDMs) also viewed Cloud services as a necessary part of doing business, but also something they'd like to impose limits upon.

Nearly a third (32%) of ITDMs saw terrorist organisations as a likely source of attack



American ITDMs are some of the most confident on tackling cyber crime

73%

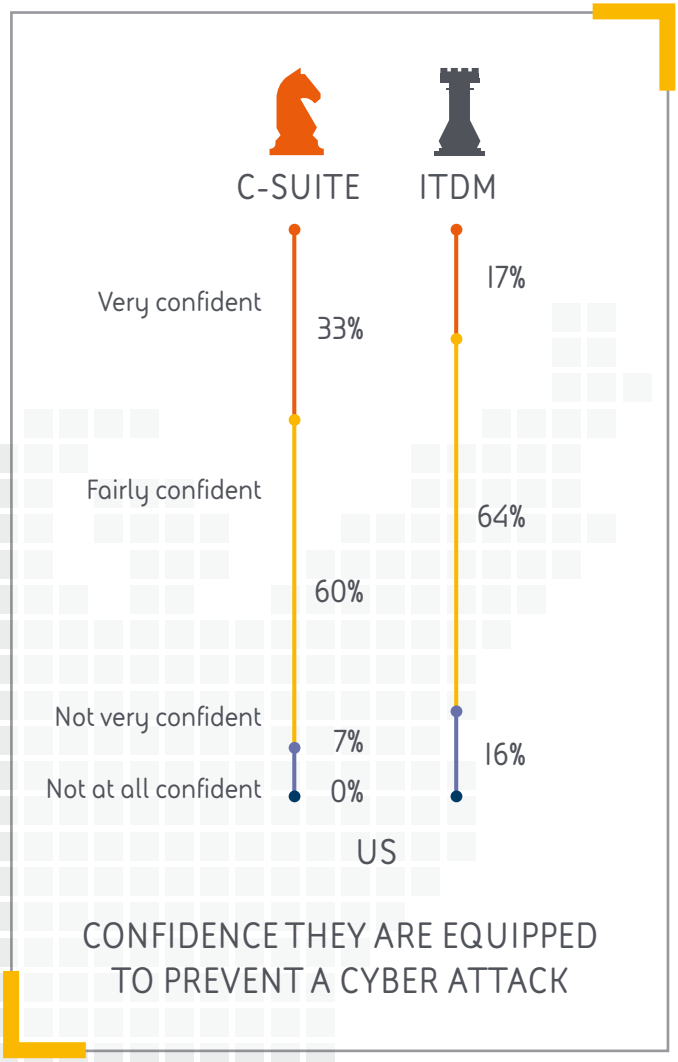
We have enough support from suppliers, enforcement agencies and government to tackle cyber security

79%

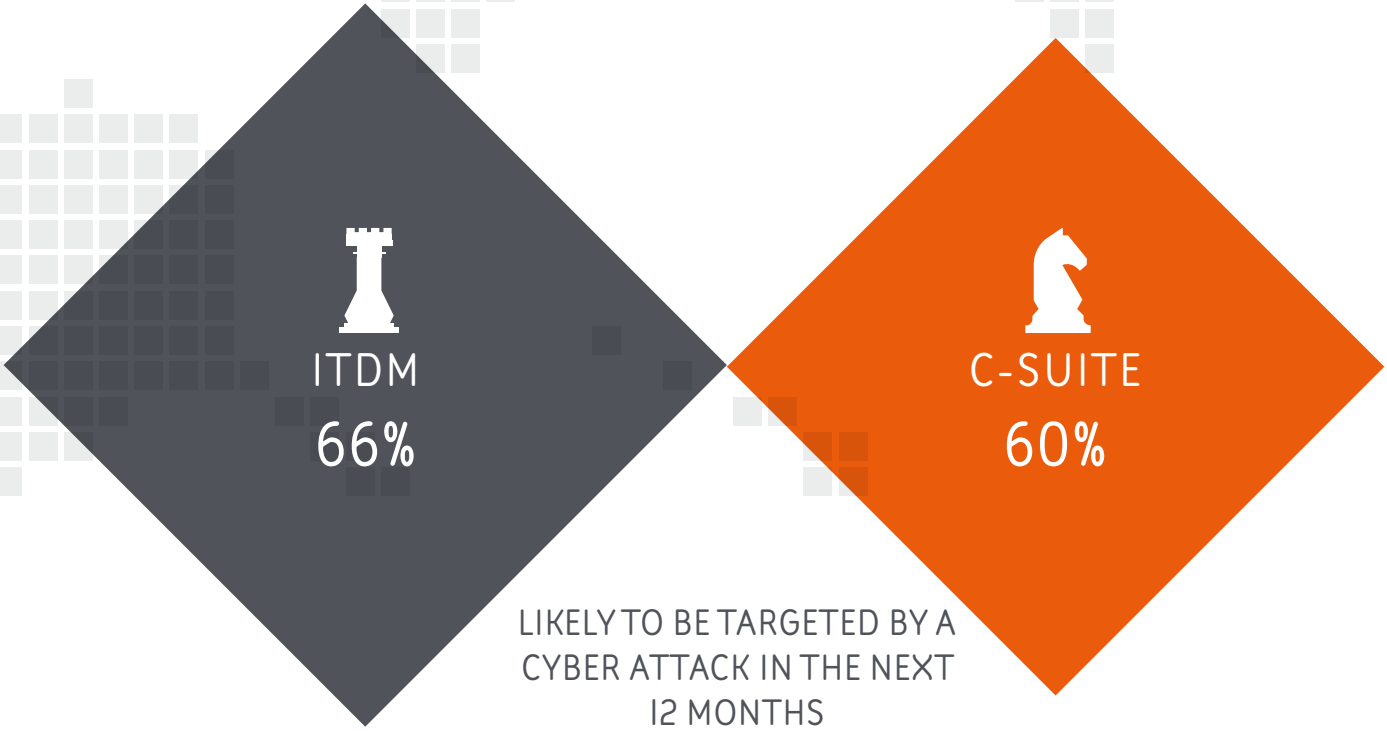
We have enough information to make informed decisions on cyber security

84%

Our board takes the risk of cyber attack seriously



CONFIDENCE THEY ARE EQUIPPED TO PREVENT A CYBER ATTACK



LIKELY TO BE TARGETED BY A CYBER ATTACK IN THE NEXT 12 MONTHS

Country view: Canada

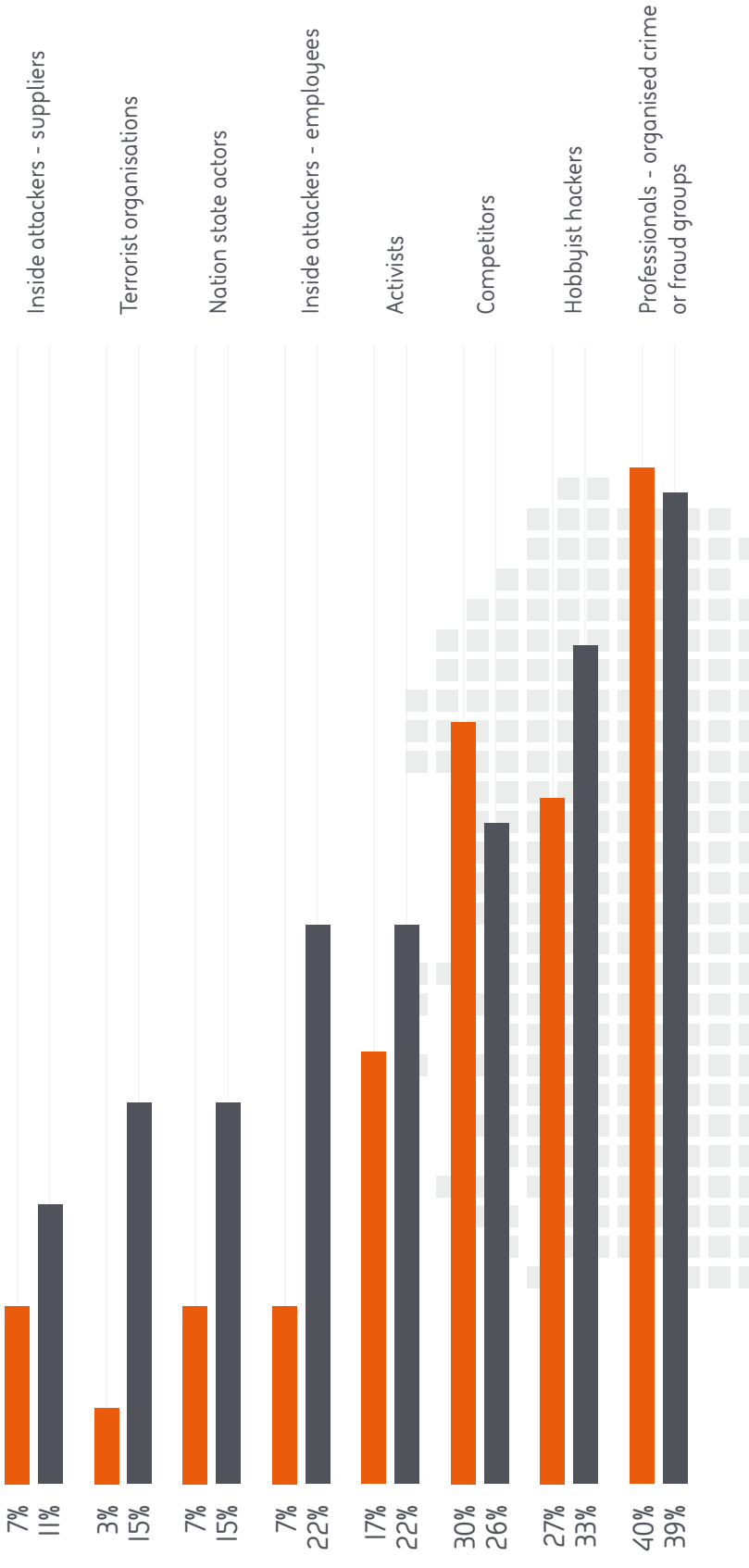
Along with Australians, and their neighbours in the USA, Canadian ITDMs and C-suite respondents rank as the most confident that their organisations are equipped to repel cyber attacks. ITDMs in Canada are also very likely to argue that their counterparts are responsible for an attack succeeding: 54% of IT Decision Makers said they thought responsibility for a security breach lies with senior management, compared to 20% of Canadian C-suite respondents who felt it was up to the IT team.

It's interesting to compare Canadian responses to those from South of the border, too. Despite this proximity, it's clear that business and technology assumptions and experiences are different enough to generate strong differences of opinion.

Canadian respondents agreed that organised crime or fraud groups posed the most likely threat, the second most likely being hobbyist hackers. This second threat stood in direct contrast to US ITDMs, who worried about cyber attacks from terror groups as their second most likely threat.

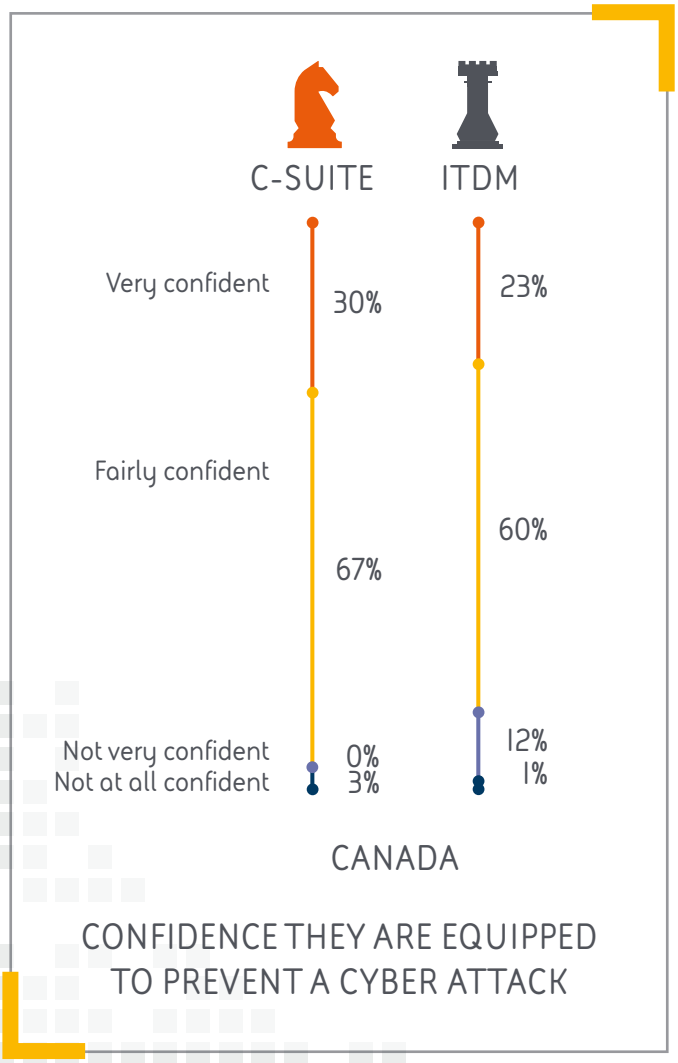
This, of course, should be tempered with a more sober assessment of the reasons for a successful cyber attack. Four out of five (80%) Canadian C-suite respondents cite human error by employees as the primary reason for a successful cyber attack. IT Decision Makers named a wider variety of reasons, with only 40% citing employee error. Interestingly, exactly half of C-suite respondents pointed towards a lack of investment in IT security as the reason for a potential breach, with a preference for blaming outdated software (43%) as the reason.

When asked for reasons as to why they would make additional investments in IT security, the answer to this problem became a little clearer. C-suite respondents talked in terms of response to new or increased cyber threats (43%) as well as plugging gaps in existing infrastructure (29%) and staying up to date with current threats (33%). In comparison, 32% of IT Decision Makers would make the investment in order to reassure customers – something only 5% of C-suite respondents put as a reason.

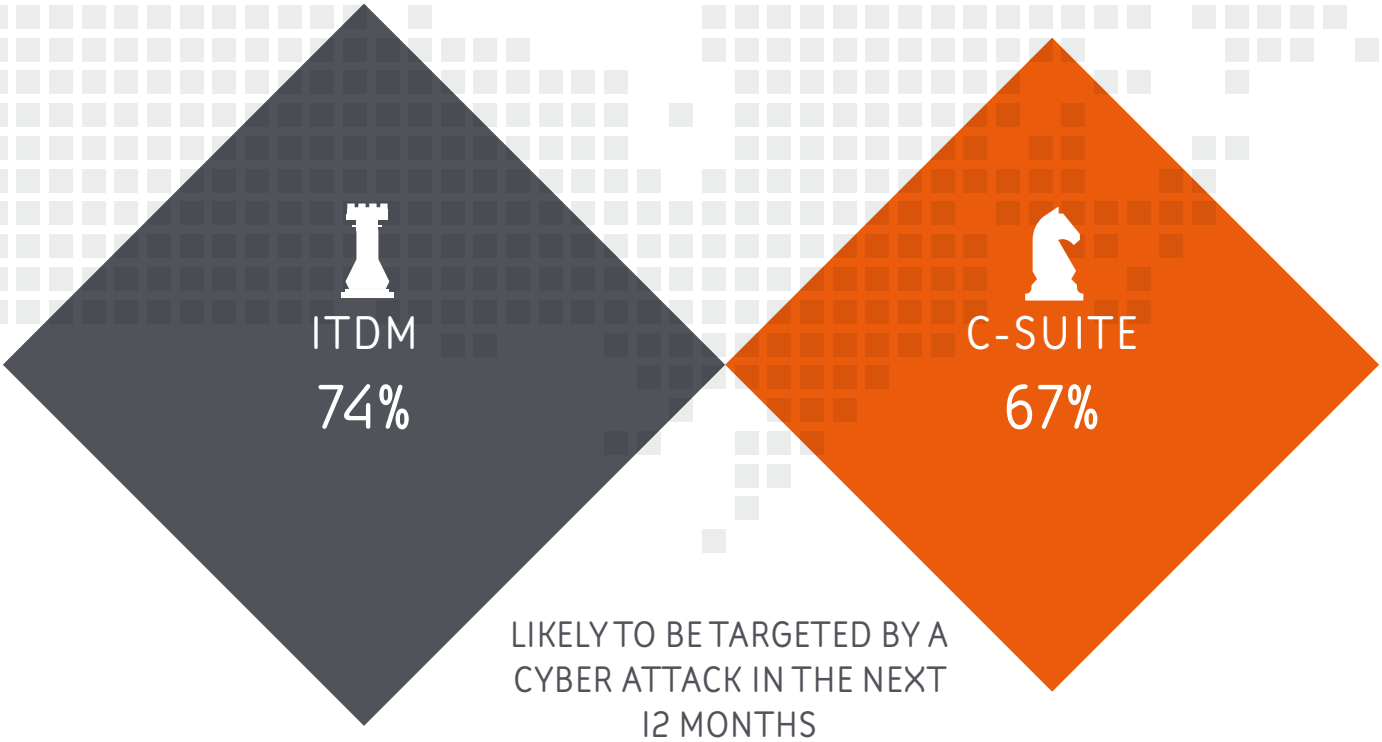


24% of C-suite respondents want more investment to help replace legacy systems

46% of ITDMs believe more investment will minimise their cyber security risk



CONFIDENCE THEY ARE EQUIPPED TO PREVENT A CYBER ATTACK



LIKELY TO BE TARGETED BY A CYBER ATTACK IN THE NEXT 12 MONTHS

We are BAE Systems

At BAE Systems, we provide some of the world's most advanced technology defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
265 Franklin Street
Boston
MA 02110
USA
T: +1 (617) 737 4170

BAE Systems
Level 12
20 Bridge Street
Sydney NSW 2000
Australia
T: +612 9240 4600

BAE Systems
Arjaan Office Tower
Suite 905
PO Box 500523
Dubai, U.A.E
T: +971 (0) 4 556 4700

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems
Level 29 Menara Binjai
2 Jalan Binjai
Kuala Lumpur 50450
Malaysia
General Enquiries: +60 (3) 2191 3000

BAE Systems, Surrey Research Park, Guildford
Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/businessdefence

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

CREST CESG Certified Service Cyber Incident Response CPNI Centre for the Protection of National Infrastructure