SPECIAL REPORT

Who Secures Europe?

AKJ Associates

HEAD OF RESEARCH
Angharad Gilbey
e: angharad.gilbey@akjassociates.com
t: +44 (0) 207 242 7820

HEAD OF CONTENT
Simon Brady
e: simon.brady@akjassociates.com
t: +44 (0) 207 430 0630

INTRODUCTION

One of the most common complaints in cybersecurity is the difficulty of getting senior management and board-level decision makers to take it seriously. Following years of increasingly high-profile data breaches, it looks like that may be about to change.

The past year has seen several significant developments. When we started working on this project it had been some time since the peak impact of WannaCry and NotPetya, but their effects were still being felt, as was the impact of high-profile breaches such as Equifax and DLA Piper. Since then, Facebook's data privacy scandals and the introduction of GDPR have increased consumer awareness of data protection issues, and mandatory disclosure regulations have led to a flood of breach reports, some of them relatively minor, and others involving millions of customers. We also saw the UK's first class-action data breach lawsuit emerge from Morrisons' payroll data leak, which was followed by suits such as those launched against British Airways and Cathay Pacific, among others.

Faced with the prospect of significantly increased fines, reputational damage, lawsuits and (perhaps most dramatically) considerable operational losses, boards are taking cybersecurity more seriously. With a clearer frame of reference for what a breach could cost them, convincing directors and management that proactive security is a worthwhile investment is a simpler task than it used to be. For reference, Ponemon put the average data breach cost in 2018 at $3.9 million,[1] while AP Moller-Maersk's NotPetya damages were estimated at up to $300 million,[2] and Equifax's at potentially "well over $600 million".[3]

But of course, I'm oversimplifying. The first issue is that 'getting budget' isn't as much like being handed pocket money as we'd like: decisions have to be justified, and with solid metrics for success still not particularly well-established in cybersecurity, proving that you're spending sensibly can be a challenge.

The second, which is really the key issue, is deciding what to do with that budget once you get it. Cybersecurity doesn't run on a coin meter – you can't just put money in and get a robust security posture out.

One question is what you want to prioritise: staff training, hiring and software solutions are the top three options, but they all come with challenges too. Training of both IT and non-technical staff (whether through a provider or done in-house) needs to be repeated frequently to be effective, but that's a lot of employee hours, and time is money. Hiring… well, we've all heard about as much as we can stand to about the cybersecurity skills gap.

As for solutions, the vendor market for cybersecurity is overcrowded to say the least.

"Since 2012, my VC friends have funded 1242 cybersecurity companies, investing a whopping $17.8bn," said Mahendra Ramsinghani, founder of cybersecurity seed fund Secure Octane, last year. "But chief information security officers say that they don't need 1242 security products. One exhausted CISO told me they get fifteen to seventeen cold calls a day. They hide away from LinkedIn, being bombarded relentlessly."[4]

1 Ponemon Institute & IBM Security, 'Cost Of A Data Breach Study'.
2 Financial Times, 'Moller-Maersk puts cost of cyber attack at up to $300M'.
3 Reuters, 'Equifax breach could be most costly in corporate history'.
4 TechCrunch, 'Lessons from cybersecurity exits'.

The other side of the problem is that while CISOs don't need 1242 products, the average cybersecurity stack *is* frustratingly complicated, with a 2017 survey indicating that the typical CISO uses as many as 50 products.[5]

Some amount of complexity is inevitable. It's no surprise that companies would have different solutions in place to deal with different issues – for example, using different products for identity and access management, email security, and traditional antivirus. No one's expecting a silver bullet solution that will secure everything – though if they are, they can find any number of providers claiming to offer one. All the same, even accounting for the varied requirements of the modern enterprise, managing fifty solutions (and fifty contracts, dashboards, and sets of patching requirements) can hardly be ideal.

"One exhausted CISO told me they get fifteen to seventeen cold calls a day. They hide away from LinkedIn, being bombarded relentlessly"

Part of the reason for the complexity is that it can be difficult to find a solution that exactly fits the company's specific requirements, with the result that several products (often with significant overlap) may be used for one task. Determining which products come closest to fulfilling the company's specific requirements can be a challenge, and the procurement process – when carried out with the diligence it deserves – is far more intensive in terms of time and labour than it needs to be. And it doesn't always work out well: according to research by Gartner, one in three IT professionals wouldn't recommend the product or service they implemented.[6]

Much of the information that's readily available about security products is marketing put out by the vendor company itself, and it's difficult to know which sources provide reliable information about the capabilities of each product and how they compare. Both from our research and independent sources, we know that end-users are concerned about whether vendors are telling the whole story about a product's capabilities.[7] This can be tested – to an extent – by a proof of concept (POC), but that can be an even more arduous process, and there's only so many POCs a team can run.

Cybersecurity professionals simply don't have the resources to continue trying solution after solution in the hopes of finding the best ones for their needs. Rather than Prince Charming finding his Cinderella, that method is likely to end up with the CISO being saddled with one (or fifty) of the ugly stepsisters – and the old-school version at that, toe-chopping and all. The amount of time and energy (let alone money) spent on compensating for and working around inefficiencies in commercially licensed software keeps an already overworked team from focusing on other responsibilities.

Anyone who's attended AKJ's conferences or private meetings in the past will know that our belief in the importance of information-sharing is the driving force behind our events, so it should come as no surprise that that's what we're advocating here too. Pooling the experiences and insights of other professionals with the same needs and priorities, and speaking frankly and in depth with vendor representatives in a non-pressured environment, are key to getting an in-depth, detailed understanding of which products are worth approaching for a demo.

5 Cisco, Cisco 2017 Annual Cybersecurity Report.
6 Gartner, LinkedIn post.
7 E.g. Gartner, 'How to Tell When Vendors Are Hyping AI Capabilities', Channel Web, 'Security vendors are 'mis-selling technology – security reseller'.

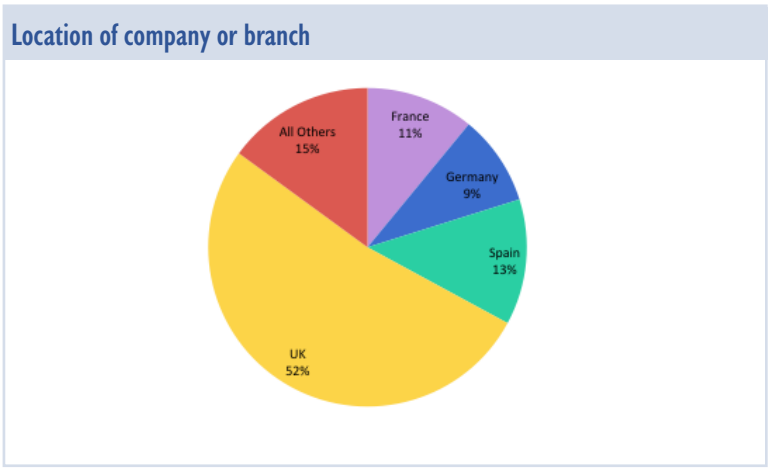
That was the drive behind the PCI Awards for Excellence, the third edition of which took place just a few months ago – results can be found here (PDF). To help bring insights of this type to a broader audience, we decided to carry out a research project in which we asked high-level professionals in cybersecurity and related fields to tell us about their experiences. We used the information they shared with us to compile this report, which gives detailed information on the challenges they face and the providers they have found most effective in addressing their specific requirements.

While no substitute for the level of in-depth insight provided by direct peer-to-peer discussion, we hope it will nonetheless be a valuable resource.

PARTICIPANTS AND THEIR CHALLENGES

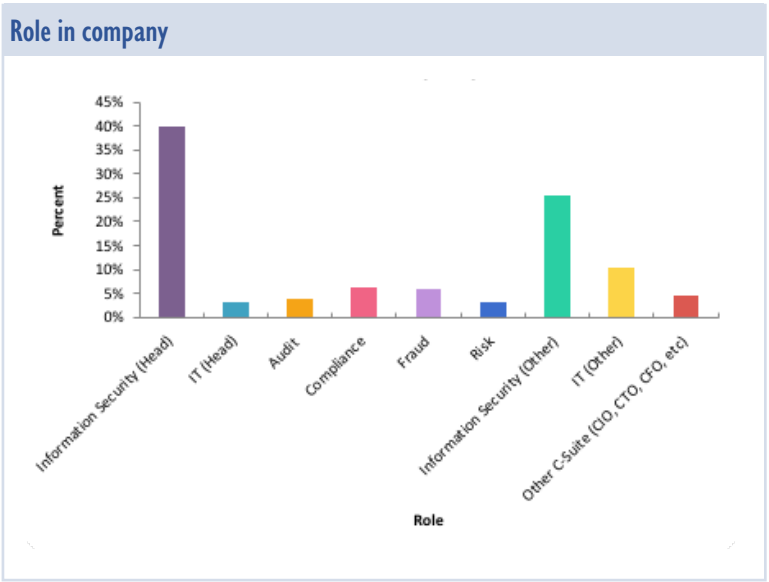
Our primary source of information in compiling this report has been an anonymous questionnaire sent out to attendees at our events in Europe and the UK.

We received over 250 responses from individuals based almost exclusively in the UK and Europe. Due to the distribution of our events, the majority of the responses we received were from the UK (52%), with a further 2% of responses coming from Ireland and the Channel Islands. The exact makeup is as follows:

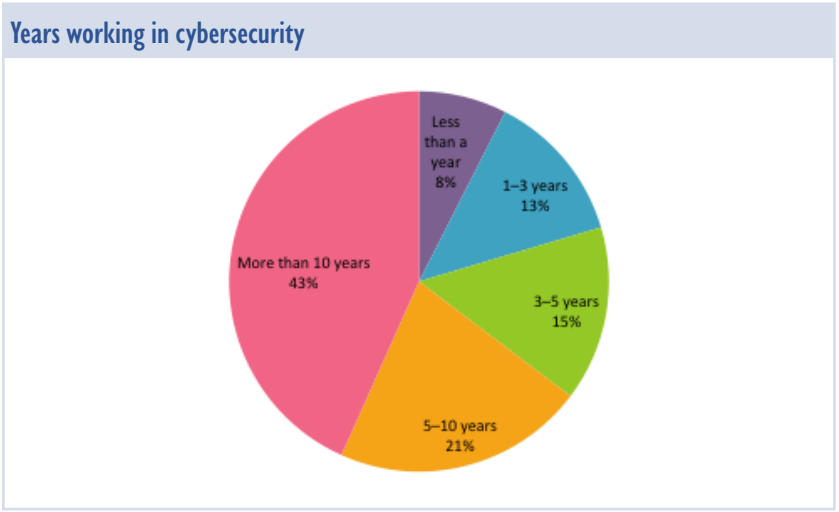


The 'All Others' category includes Austria, Belgium, Bulgaria, the Channel Islands, Denmark, Finland, Ireland, the Netherlands, Norway, Serbia, Sweden, and Switzerland. It also includes one response each from Morocco, Tanzania and the USA, though these participants' attendance at our European events suggests they operate in the region to some extent.

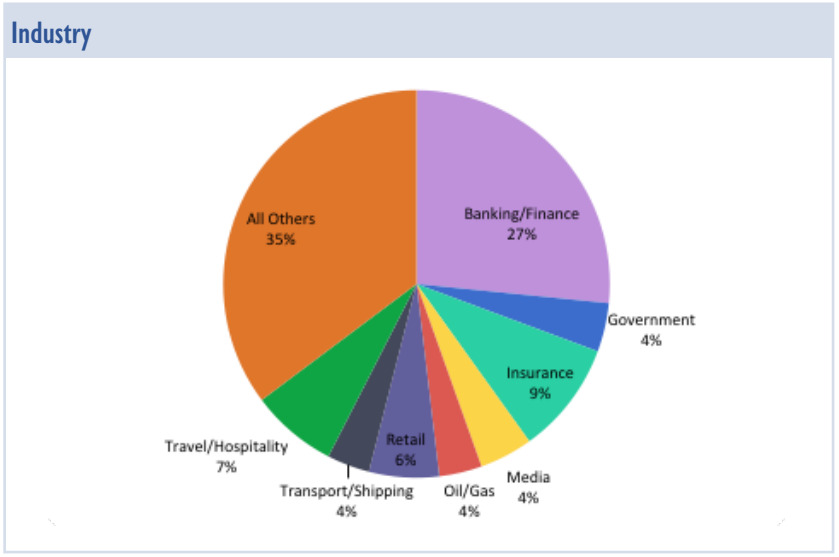
All participants deal with IT security and infrastructure at end-user organisations, the majority being specifically responsible for information security. Though the length of their experience specifically in cybersecurity varies – given the much-discussed skills gap, recruiting from other strategic, governance or technology roles is standard – they are typically senior representatives with influence (direct or otherwise) on security decision-making:



Participants who reported less than a year's experience in cybersecurity all specialised in other areas, mostly compliance or non-security IT roles



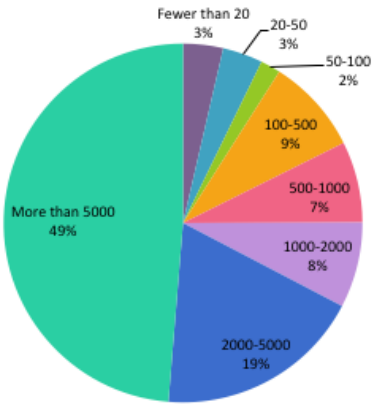
They represent a variety of organisations in different industries, though financial organisations – unsurprisingly – are particularly well-represented:



'All Others' includes electronics/telecommunications, business services, charity, education, health/pharmaceuticals, construction/engineering, law enforcement, food/beverages, utilities, real estate, mining, aerospace/defence, conglomerate, and research.

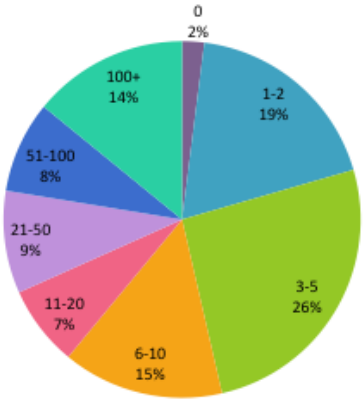
Participants also represent a range of company sizes. Again, due to the typical makeup of our delegation (and the type of company likely to have teams or individuals whose specific remit is cybersecurity), there is a much larger proportion of large than small companies represented, with the majority having over 5000 employees:

Number of employees



We also asked some questions to gauge the organisation's commitment to and investment in information security, both for 'demographic' purposes and because they are interesting in their own right:

Number of people in the company's information security team



For every size band except '5000+ employees', infosec teams most commonly had 5 members or fewer

Because of the difference in company sizes, this graph may be more illuminating when compared with company sizes:

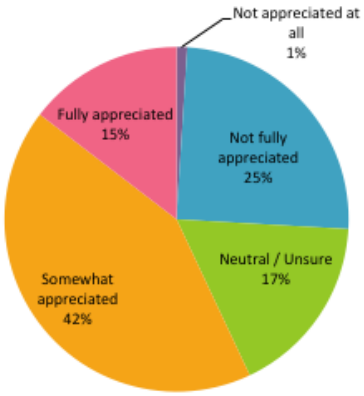
Number of employees in company vs. size of information security team

	Lowest	Highest	Mean	Most common
Fewer than 50	1-2	6-10	3	3-5
50-100	1-2	11-20	7	1-2
100-500	0	100+	9	1-2
500-1000	1-2	21-50	5	1-5
1000-2000	1-2	100+	35	3-5
2000-5000	0	100+	37	3-5
5000+	0	100+	214	100+

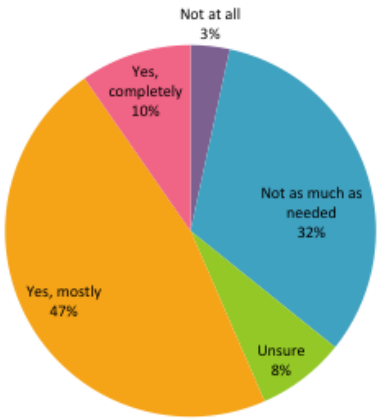
'0' only appears in medium to large companies, which are at the very least invested enough in information security to send a representative to one of our events. This may indicate that while the individual responding holds responsibility for information security, security operations are outsourced rather than having a team in-house.

Over a third of participants said their infosec team didn't have the board-level support it needed to operate effectively

Board appreciation for CISOs' knowledge about operational risk



Sufficient board support to defend against threats



Overall, though the proportion who indicated that the board was fully 'on board' is low, the majority of participants in the poll were reasonably happy with the level of support they received from the board. Despite this, most reported fairly small information security teams – even though almost half of our participants said their company had over 5000 employees, less than a third said that the company's information security team numbered 20 or more.

While teams may be supported by a complex infrastructure of technical solutions, and perhaps outsourcing or automation of some tasks, this remains slightly worrying. In a 2017 survey, under half the participants reported that their security teams were fully staffed, and only a third said they had the mix of skills needed to combat threats they anticipated facing in the year ahead.[8] Our findings certainly seem to reflect that as well.

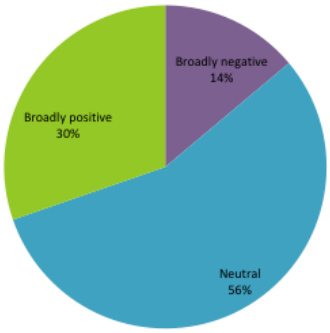
8 Dark Reading, 'Surviving the IT Security Skills Shortage'.

THE STATE OF THE SOLUTIONS MARKET

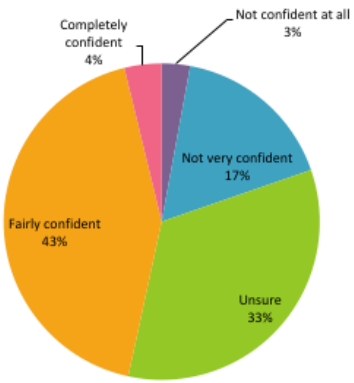
Our demographic questions revealed some interesting trends themselves, particularly relating to levels of board support and staffing, which we are keen to explore further in future. However, the main purpose of this research project was to explore IT and information security professionals' thoughts on the vendor marketplace. One of the primary areas we looked at is how end-users feel about the current marketplace for security solutions, and where they think improvements need to be made.

The first questions we asked were fairly broad:

Overall view of cybersecurity vendor ecosystem

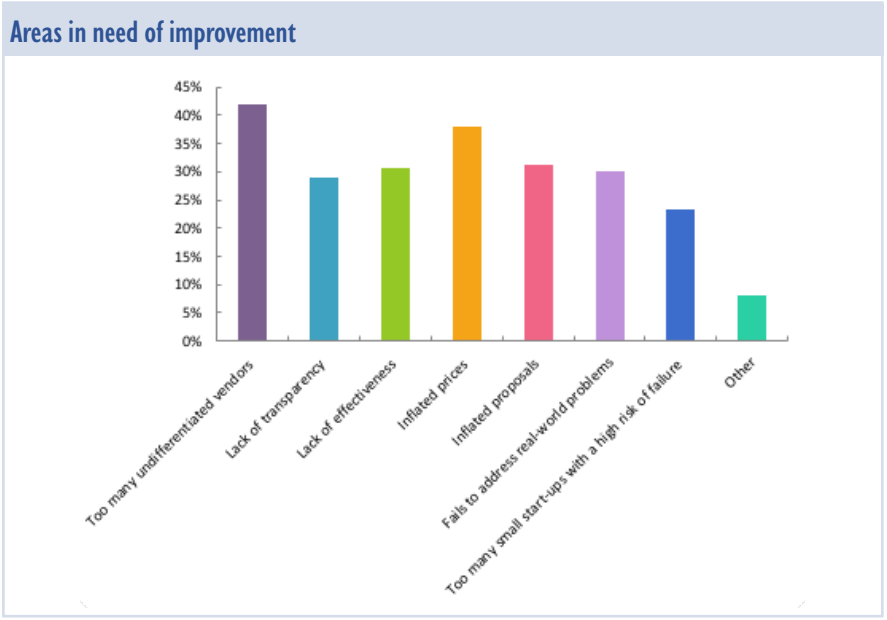


Confidence in reliability of easily-available information about solutions and providers



Fewer than half of participants were confident that the information readily available about cybersecurity solutions was reliable

Whether they reported a positive, neutral or negative perspective, we also asked participants to tell us which aspects of the cybersecurity vendor ecosystem they considered most in need of improvement:



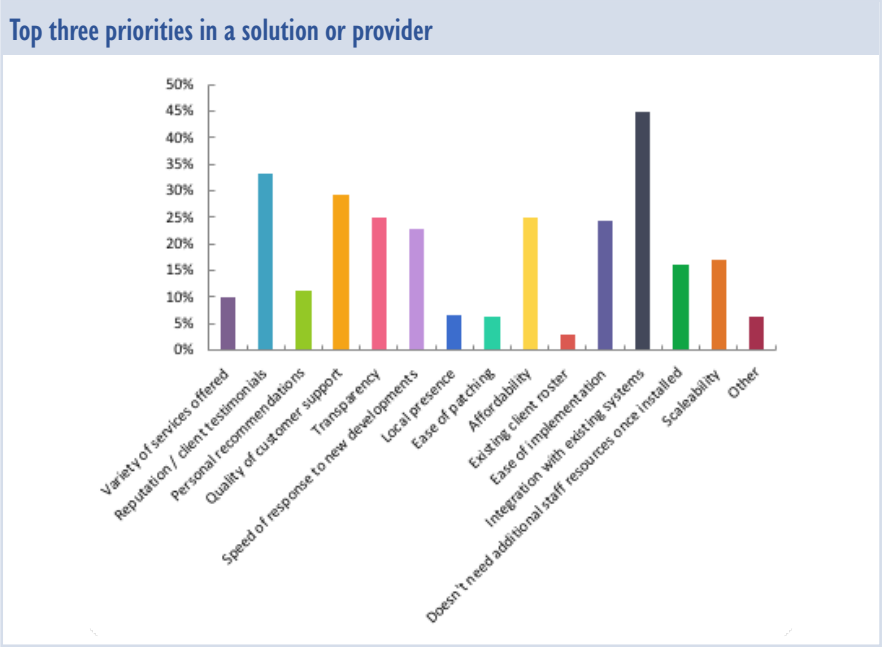
For 'Other', participants wrote in their own answers. Almost a full third of participants who did so told us that bandwagons such as GDPR were the main problem, all using the term 'bandwagon' and specifying GDPR as an example. Given that many of the responses to our survey were submitted during the months surrounding May 25th 2018, this issue may have been weighing particularly heavily on participants' minds. However, GDPR is hardly the only bandwagon around in cybersecurity - blockchain and AI are other examples which spring to mind. While all are highly relevant to cybersecurity professionals, there's no denying that they've been surrounded by significant hype.

Another problem cited by several of these participants (though with slightly less uniformity) was a lack of clarity – again, cited by roughly one third. Implementation timelines, staffing requirements, how to deploy the solution, and post-deployment processes were all cited as issues.

The remaining 'other' answers included 'too much focus on solving point problems', 'selling "solutions" by inventing problems', the difficulty of integrating multiple solutions, the fact that many solutions overlap in terms of functionality (leading to redundancies and alert fatigue), and the number of separate and distinct solutions needed, most of which have to be obtained from different providers.

Another referred to vendors being more focused on trying to outsell their competitors than on actually providing the best possible solution, and one (taking a perhaps controversial stance) suggested the primary problem was 'TOO MANY OVER 50's in senior positions', which the participant believed resulted in difficulty keeping up with such a rapidly changing marketplace.

Looking at the issue from a different angle, we also asked participants to tell us their top three priorities in a solution or solution provider:



'Integration with existing systems' is the top priority by a considerable margin – not surprising considering the complexity of most companies' IT infrastructure

'Other' answers here included ease of customisation ("everything in this field requires bespoke tuning", one participant added), real-world applicability, proven knowledge and experience of the provider, and independent confirmations of effectiveness.

Approximately half of the 'other' answers, however, boiled down to 'the product actually works'. This was not included as an option as we assumed this would go without saying – but apparently our participants felt otherwise.

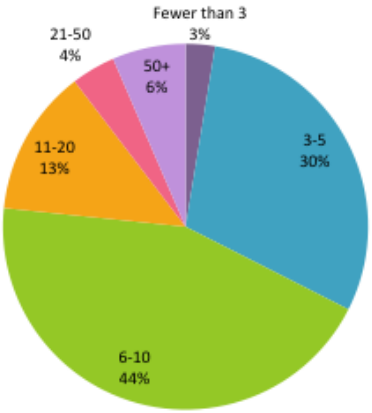
Overall, these responses match up fairly well with responses regarding the problems in the market. 'Integration with existing systems' as the top priority is unsurprising, given the need in most cases to have a fairly significant number of security solutions running in tandem (let alone all the rest of the company's software/hardware infrastructure). 'Reputation / client testimonials' and 'personal recommendations' reflect concerns about a solution's reliability, and 'quality of customer support' is crucial when staff resources are already stretched.

The difference between how many considered 'inflated prices' a top problem, and the significantly smaller proportion who said 'affordability' was a top priority, suggests that with so many other factors affecting product choice, perceived overpricing may be something CISOs have to simply grin and bear.

Based on Cisco's report that the typical CISO uses up to 50 separate security solutions, we were curious as to whether our participants would report the same:

Some participants said they were using 50+ distinct solutions, but most were using 10 or fewer

How many distinct solutions do you currently use in your cybersecurity stack?

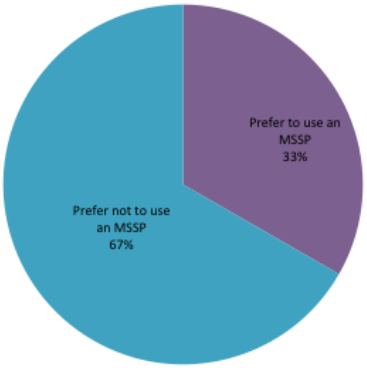


'Up to 50' is borne out by our findings – 6% of participants even reported using more. However, both Cisco's research and our own found that the majority of participants were using far fewer. Most of their participants (64%) said they used 10 products or fewer in their security environment, with 35% reporting 5 or fewer.

As can be seen from this chart our own findings were extremely similar, though participants in Cisco's survey seemed to have larger information security teams (only 15% said that their company employed fewer than 10 security professionals), indicating a higher ratio of staff members to products.

Given that staff shortages and integration difficulties were issues for our participants, and responses to the above question indicate many teams had more products than members, we were curious as to how participants might feel about Managed Security Service Providers (MSSPs). We expected to see a fairly even split in results, but two thirds of participants said they would prefer not to use an MSSP:

Preference for use of MSSPs

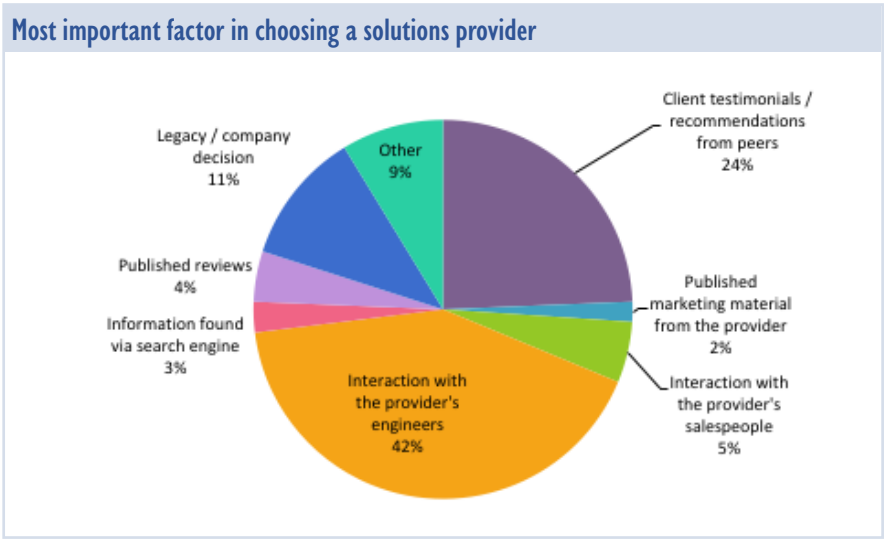


We did give participants the opportunity at the end of the survey to provide additional comments, but none commented regarding the pros and cons of using an MSSP.

However, in our Middle Eastern version of the survey (which produced a much more evenly split vote), we received several unprompted comments on the drawbacks of MSSPs, with multiple participants mentioning that they would place less trust in an MSSP than an in-house team.

Part of this came down to not wanting (or being forbidden by regulation or policy) to open themselves up to the risk of a breach or leak occurring via the MSSP – several of 2018's big data breaches were caused by supply chain attacks, including on software companies. Companies may simply be unwilling to take the chance of giving a third party that much access.

As well as asking participants about their priorities, we also asked which resources they relied on to evaluate whether specific vendors managed to fulfil those priorities:



The top factors by far were interactions with engineers and client testimonials - CISOs need confirmation that products work as advertised

Most 'Other' answers said that the proof of concept (POC) process was the most important factor. These should, in our opinion, be counted along with 'interaction with the provider's engineers', a category which we certainly intended to include POCs and demos. In that case, the category would account for almost exactly 50% of votes.

The other 'Other' answers included references to tendering (a legal requirement for some organisations), slightly enigmatic answers such as 'knowledge' and 'experience' (perhaps indicating personal experience with the product or provider while at another organisation), and my personal favourite: 'They seemed ok'.

While a POC is invaluable for ruling out solutions which clearly won't be fit for purpose, it can be hard to judge the long-term experience from a single POC, as some participants commented earlier. Teams are still likely to end up with a list of solutions which perform at least adequately in a POC, meaning that further differentiation is required - though of course we wouldn't expect anyone to overlook an unsuccessful POC in favour of a good experience with a salesperson, it makes sense that reviews and recommendations are also mentioned frequently as deciding factors.

The relatively high proportion who responded with 'legacy/company decision' also makes sense. Replacing a piece of software or hardware can be even more complicated than installing it in the first place – so given the high employee turnover in information security, even at a senior level, software may well outlast personnel. And with regards to company decisions, while it's unlikely that a cybersecurity purchasing decision would be made without consulting the relevant team, other parties may have ultimate control over which of the options proposed by the CISO is chosen.

Because we anticipated 'interaction with engineers' receiving a high proportion of votes due to the importance of the POC process, we also asked participants to rank how important the various other factors were to their decision. That produced the following chart:

Item	Overall rank	Rank distribution
Client testimonials/recommendations from peers	1	
Interaction with the provider's engineers	2	
Published reviews	3	
Interaction with the provider's salespeople	4	
Information found via search engine	5	
Legacy/company decision	6	
Published marketing material from the provider	7	
Other	8	

Approximately one third of 'Other' answers cited POCs again. Other 'Other' answers included responses to bid documentation (with one again specifying tendering), and 'ease of escalation if necessary', which would perhaps be a better fit for the question about priorities in a vendor.

Overall, answers to both parts of this question show that the major factors in decision-making are direct interaction with engineers (often, though not necessarily, during the POC process), and independent confirmation via published testimonials or peer recommendations. Unfortunately, recommendations and testimonials which are both reliable and relevant to a company's specific needs can be hard to source.

That difficulty is part of what inspired this project, so at the very least, it's gratifying to see our thinking confirmed – and hopefully we'll also be able to help address it.

WHO STANDS OUT?

The findings of the previous chapters confirm what we have heard over and over from CISOs. They're struggling with the saturated solutions market, and have trouble cutting through the sheer volume of marketing blurb and sales pitches to determine which product can best address their needs. To help ease this process, we asked our participants to tell us which vendors they had found particularly effective, both in terms of fulfilling their priorities and in specific areas of security risk.

Overall, the thirty vendors most frequently mentioned by our participants, including responses to all questions, were as follows:

1	McAfee
2	IBM
3	Cisco
4	Proofpoint
5	Dell
6	Palo Alto Networks
7	Symantec
8	FireEye
9	Trend Micro
10	Micro Focus
11	Splunk
12	Check Point Software Technologies
13	Orange Cyberdefense
14	Mimecast
15	Sophos
16	Microsoft
17	NCC Group
18	AlienVault
19	BlackBerry
20	CrowdStrike
21	Forcepoint
22	Cyber-Ark Software
23	Darktrace
24	Nettitude
25	ECSC
26	MobileIron
27	Fortinet
28	4iq
29	Blackfoot
30	Digital Shadows

The adage 'nobody ever got fired for buying IBM' comes to mind: large, big-brand, one-stop-shop providers top the table

Votes for providers whose parent companies also provide IT and cybersecurity solutions are included under the parent's name, even if they currently operate semi-autonomously – for example, votes for Blue Coat Systems and Message Labs are included under Symantec, votes for Cylance are included under BlackBerry, and votes for SecureData are included under Orange Cyberdefense.

This list tracks total mentions of a vendor, rather than the number of participants who mentioned them at least once, so in many cases a participant will have 'voted' multiple times for the same vendor. Vendors whose services cover a wide range of risk areas are therefore in a position to receive more 'votes' than those offering or specialising in more niche services.

This makes for a particularly interesting comparison with the responses to our first specific question about vendors, in which we asked participants which three vendors fulfilled their priorities most effectively. What this specifically means for each vendor therefore varies based on the participant's priorities. A more detailed breakdown of how priorities map to specific vendor nominations can be found on p19 of this report, but we would expect those ranked highly overall to be reasonably consistent with the overall top few priorities: integration with existing systems, reputation / client testimonials, quality of customer support, affordability, and ease of implementation being the top five.

Moreover, if a participant tells us that these vendors are the best at fulfilling their priorities, then regardless of what these priorities are, we can assume that these are the vendors with whom they would be most inclined to work.

The top thirty vendors named in this category are:

Again, big names come out on top, but there's a little more diversity here. Note the presence in the top 10 of relatively young providers like CrowdStrike, and more specialised ones such as Mimecast

1	McAfee
2	Palo Alto Networks
3	Cisco
4	FireEye
5	IBM
6	Proofpoint
7	Trend Micro
8	CrowdStrike
9	BlackBerry
10	Mimecast
11	Sophos
12	Symantec
13	Fortinet
14	Dell
15	Qualys
16	Akamai
17	Micro Focus
18	Microsoft
19	Splunk
20	Tenable Network Security
21	Varonis Systems
22	AlienVault
23	Blackfoot
24	DXC Technologies
25	Cyber-Ark Software
26	Deloitte
27	Digital Shadows
28	ESET
29	Flashpoint
30	Forcepoint

As can be seen, the two tables are for the most part very similar, though it's interesting to note the companies which do markedly better in one than the other.

Finally, we also thought it would be valuable to sort companies in terms of the number of unique voters they received across all areas:

1	Dell
2	Proofpoint
3	McAfee
4	Cisco
5	Symantec
6	FireEye
7	IBM
8	Palo Alto Networks
9	Splunk
10	Check Point Software Technologies
11	Trend Micro
12	Micro Focus
13	Darktrace
14	AlienVault
15	BlackBerry
16	CrowdStrike
17	Cyber-Ark Software
18	Forcepoint
19	Microsoft
20	Mimecast
21	MobileIron
22	Kaspersky Lab
23	NCC Group
24	Pen Test Partners
25	Akamai
26	Fortinet
27	LogRhythm
28	Sophos
29	Deloitte
30	Digital Shadows

Dell, ranked in the top 15 in both previous tables, takes first place here due to the strong performance of products such as SecureWorks in specific risk categories

Big names still dominate in this category, as they do in all of these charts, primarily because they offer a greater variety of services and so can be named in more categories. However, it's interesting to see that this table is less similar to the previous two than they are to each other, with some companies – particularly newer companies or those with one (or more) highly focused products – doing markedly better here. For example Dell, which did well overall but takes a higher place in this table, did so in significant part due to the many participants who mentioned its products in just one or two specific defence categories.

In all vendor-related questions, we asked that participants write in 'None' if they felt that no vendor particularly stood out from the crowd. Overall, 'None' was by far the most frequent answer (though this is somewhat distorted by the high proportion of responses in categories such as 'IoT security'). This doesn't necessarily mean that no vendor was thought to be effective at all – if it did we would expect a much higher proportion of participants to have reported a negative perception of the vendor ecosystem – but it likely reflects the difficulty of differentiating between vendors.

Apart from this question, the other major source of 'mentions' used to compile the first list was a question in which we asked participants to tell us about the provider they considered most effective in specific areas of cybersecurity. It's all very well buying from a vendor with a good overall reputation, or whose other solutions you've found effective in the past, but they won't be 'best in breed' in every area there is. Organisations need to be aware of the threats they're vulnerable to, and they need to choose their solutions accordingly.

77% of responses in the IoT security category said that no vendor stood out as particularly effective

Risk/service Area	Most effective
Network security	Cisco
Threat management / intelligence	Digital Shadows / McAfee [tie]
SIEM / real-time threat analytics	Splunk
Endpoint security	McAfee
Email and messaging security	Proofpoint
Web security	Symantec
Incident response	IBM
'Internet of Things' / Industrial / SCADA security	None (11 providers nominated)
Mobile device security	Dell
Payment / transaction / e-Commerce security	WorldPay
Identity and access management (IDAM)	Cyber-Ark Software
Penetration testing	Pen Test Partners
Cybersecurity training	SANS
Managed security service provider (MSSP)	IBM / Dell [tie]

Only a few categories were won by the same provider in both the UAE and European versions of our project. These were Cisco in the network security category, Splunk in the SIEM category, and Symantec in the web security category.

While in most categories there is a clear standout 'winner', in others the competition is considerably closer. This is particularly true of the 'IoT security' category, which received only eleven votes, all for different companies. Many of our participants didn't answer the question at all (perhaps due to lack of familiarity with the market for IoT security solutions), but 77% of those who did wrote in 'None'.

The 'payment security' category experiences something similar – WorldPay does emerge as a winner, but 64% of participants wrote in 'None', and several participants did not respond, probably for the same reasons as in the 'IoT security' category. In other categories, such as the 'threat management/intelligence' category, we received plenty of responses but still found the competition for the top spot was quite close, resulting in ties.

On the other hand, responses to other categories did show clear favourites. Proofpoint, for example, stood out as a clear winner in the 'email and messaging security' category, winning 22% of all votes (and 28% of the votes which named a vendor). Dell, the winner in the

'mobile device security' category, also stood out considerably beyond its nearest competitor, accounting for 23% of all votes (and 35% of the votes which specified a vendor).

It should be noted that all Dell votes in the 'mobile device security' category specified AirWatch, a VMware product, rather than naming the company more generally. Likewise, in the MSSP category, all products referred to Dell SecureWorks in particular, with some leaving out the 'Dell' brand.

As well as effectiveness in different risk areas, we think that one of the most important insights our research can offer is how other priorities affect vendor choice. For individuals with the time to do so, going through marketing material and published reviews, speaking to senior vendor representatives directly, and running POCs can give a fairly good sense of the solution's ability to meet technical criteria. The information that's harder to get hold of is how vendors compare in terms of priorities which are more strategic or business-oriented than technical.

Participants were each asked to specify three priorities, and three vendors who best fulfilled these. It should be kept in mind that we did not ask participants to specify (for example) which vendor they considered most transparent. However, as we observed some clear trends standing out, we thought these results were worth including here.

Priority Order	Priority	Best fits priorities	Most mentioned
1	Integration with existing systems	McAfee	McAfee
2	Reputation / client testimonials	FireEye	FireEye
3	Quality of customer support	FireEye	IBM
4	Affordability	FireEye	Sophos
5	Transparency	Cisco	Orange Cyberdefense
6	Ease of implementation	Symantec	McAfee
7	Speed of response to new developments	McAfee	IBM
8	Scalability	Palo Alto Networks	IBM
9	Lack of need for additional staff resources	McAfee	Proofpoint
10	Personal recommendations	Cisco	IBM
11	Variety of services offered	Palo Alto Networks	Dell
12	Local presence	IBM	IBM
13	Other (please specify)	Accenture	Accenture/BAE Systems/ Digital Shadows/Proof-point/Splunk [tie]
14	Ease of patching	Consist/McAfee/Micro Focus/ Palo Alto Networks [tie]	Palo Alto Networks
15	Existing client roster	Deloitte/McAfee (tie)	Verizon

From number 13 down ('Other'), relatively few participants had selected these priorities, resulting in several ties.

Cisco was the only provider which won the same category in both the European and UAE versions: it was voted the best fit by participants who selected 'transparency' as one of their top three priorities. Symantec, voted the best fit for those who prioritised 'ease of implementation' in the European version, was the most frequently mentioned by participants who selected this in the UAE version.

We also found that more 'demographic' factors such as industry, region and company size made a difference, as did job-related factors such as role, level of board support, and size of information security team.

'Actually no one' – health sector participants in both the European and UAE polls say solution providers are not meeting their needs

Industry	Best fits priorities	Most mentioned
Banking/Finance	CrowdStrike	IBM
Public sector	Palo Alto Networks	Palo Alto Networks
Education	Blackfoot	Blackfoot
Legal	Mimecast	Mimecast
Retail	FireEye	McAfee / FireEye [tie]
Travel/Hospitality	DXC Technology	McAfee
Healthcare/Pharmaceuticals	No vendors named	No vendors named
Insurance	Varonis Systems	Check Point Software Technologies
Telecommunications	Cisco	Cisco
Manufacturing	BlackBerry / Proofpoint [tie]	4iQ
Oil/Gas	McAfee	Check Point Software Technologies/ Symantec [tie]
Charity	Nettitude	Nettitude
Other	BlackBerry	Dell

Two categories had the same 'winner' in both the European and UAE versions. One of these was the oil and gas industry's choice for 'best fits priorities', where they selected McAfee. The other was the healthcare sector's response to 'best fits priorities' – in both versions, participants did not name any vendor as fitting their priorities, with the only response in either version being 'actually no one'.

Region	Best fits priorities	Most mentioned
UK, Channel Islands & Ireland	FireEye	Dell
Germany, Austria & Switzerland	Proofpoint	Proofpoint
France	Palo Alto Networks	Palo Alto Networks
Spain	IBM	McAfee
Benelux	Cisco/Palo Alto Networks [tie]	IBM
Scandinavia	Cisco	Cisco/Thinkst Canary/Yubico [tie]
Other	CrowdStrike/Flashpoint [tie]	CrowdStrike

Members in infosec team	Best fits priorities	Most mentioned
0	Fortinet	Cisco
1-2	Mimecast	McAfee
3-5	McAfee/Cisco [tie]	McAfee
6-10	FireEye	FireEye
11-20	IBM / Symantec / Proofpoint [tie]	IBM
21-50	DXC Technologies	IBM
51-100	FireEye	IBM
100+	McAfee	Dell

Role	Best fits priorities	Most mentioned overall
CISO/equivalent	Palo Alto Networks	McAfee
Infosec (other)	FireEye	IBM
IT Director	Mimecast	Mimecast
IT (other)	McAfee	McAfee
Audit	Cisco	Cisco
Compliance	Proofpoint	ECSC
Fraud	Accenture	Accenture/Digital Shadows [tie]
Risk	McAfee/Proofpoint [tie]	McAfee
Other C-suite (CIO, CTO, CFO, etc)	BlackBerry	Orange Cyberdefense

Audit professionals in both the European and UAE versions of this project gave Cisco a win in both categories. Apart from this, there is little similarity between results.

Years in cyber	Best fits priorities	Most mentioned
Less than a year	Forcepoint/McAfee [tie]	Forcepoint/McAfee/Mimecast [tie]
1-3 years	Cisco	McAfee
3-5 years	Palo Alto Networks	Palo Alto Networks/Dell [tie]
5-10 years	Palo Alto Networks	Symantec
More than 10 years	McAfee	IBM

Symantec was the most mentioned company by those with 5-10 years' direct experience in both the UAE and European surveys, and in the 1-3 years category Cisco was voted the best fit for priorities by participants in both versions. Cisco was in fact extremely popular across all levels of experience in the UAE version – it was only the 'less than a year' category in which Cisco did not win either 'best fits priorities' or 'most mentioned'.

Top factor in procurement decisions	Best fits priorities	Most mentioned
Client testimonials/ recommendations from peers	McAfee	FireEye/IBM
Published marketing material	Proofpoint	Proofpoint
Interaction with salespeople	Sophos	Sophos
Interaction with engineers	McAfee	McAfee
Information found via search engine	Orange Cyberdefense	Orange Cyberdefense
Published reviews	Symantec	4iQ
Legacy/company decision	DXC Technologies/Palo Alto Networks/SentinelOne	Dell
Other	Cisco	IBM

While big brands claimed the top 3 places, the diversity in Top 30 companies (particularly compared to the UAE report) seems to suggest a more mature market, which allows companies to consider their specific needs more carefully when designing their security architecture

In our UAE-specific version of this research project, we saw the same few names from the overall top 5 emerge as the winners in almost every category. While the overall top 5 were inevitably also frequent winners in the European version, we see substantially more variety here.

Given the relatively small number of vendors with a strong presence in the UAE, and the high importance placed on reputation and consistent quality of support, it's fairly predictable that a small group of vendors should dominate the market. This is especially the case given the tendency for large companies to acquire smaller competitors – votes for products such as Blue Coat and MessageLabs were responsible for a not-insignificant number of Symantec's votes in the UAE version of the poll.

The tendency to diversify through acquisition was also reflected by votes accrued in the European version – for example, IBM voters often specified IBM Resilient or QRadar, while several voters named HP Arcsight or HP Security Voltage, both of which were by that time owned by Micro Focus. And of course, the top spots are still dominated by big names, McAfee being a prime example.

However, the fact that more specialised companies (such as Proofpoint, which provides a range of services but is most commonly thought of as an email security company) and relatively young companies (such as CrowdStrike or Cylance - votes for the latter made up a substantial portion of BlackBerry's nominations) do so well in the European version is worth mentioning. So too is the fact that we see more variation in choices between different 'groups' (whether that's on the basis of industry, company size or other factors).

The banking and finance sector, consistently targeted by cybercriminals using advanced, sophisticated methods, chose CrowdStrike, a provider of next-gen endpoint protection, threat intelligence and incident response. On the other hand, the education sector (dealing with high numbers of users accessing sensitive data) picked Blackfoot – best known for training and consultancy – while the legal sector (particularly heavily targeted by phishing and business email compromise scams) picked email security provider Mimecast.

This seems to reflect a more mature market, in which a wider variety of solutions are easily available, and can generally be deployed with more confidence due to greater on-the-ground presence. This allows companies to consider their specific needs more carefully when designing their security architecture, rather than simply implementing the 'basics'.

Competition keeps the marketplace innovating, rather than allowing vendors – and end-users – to get complacent. The greater variety of solution types (whether that's in terms of the area they focus on, such as email, or the methods they use, such as behavioural analytics) also allows users more freedom to create the security stack which best suits the specific risks they face.

Developing a cohesive and tailored information security strategy featuring behavioural as well as technological solutions is of course more important than having the most or newest or shiniest toys. But given the complexity of securing every endpoint and defending against all threats and attack vectors, the oft-quoted adage of 'defence in depth' (cited by our participants as well) has much to recommend it.

CONCLUSION

An unfortunate truth of cybersecurity is that organisations have to cover all their bases, while a threat actor only needs to find one exploitable vulnerability.

Once upon a time, the vast majority of the gaps in a company's defences could be plugged or compensated for by a combination of a firewall and an antivirus programme. As attack vectors, strategies, and deliverables such as malware all become more advanced, many companies are finding themselves with exponentially-growing shopping lists for solutions capable of keeping the criminals out and data (and money) in.

Responses given by participants in our project corroborated what other sources had reported – cybersecurity stacks are becoming ever more complicated, with cybersecurity professionals using separate products for each of a wide range of tasks.

With cybersecurity teams themselves mostly understaffed, and over a third of participants reporting insufficient board support, this growth is not sustainable, and can even introduce new problems of its own. Cybersecurity professionals who've over-prioritised technological fixes when allocating budget will feel it elsewhere (for example, in hiring or in training costs), and for their pains, they're likely to end up with either alert fatigue or shelfware.

And that's if the product they've bought even sticks around. One of the issues in such a fast-developing marketplace is that stability isn't guaranteed – companies are constantly being bought or sold, acquiring board members and stakeholders with differing views on strategy, or even going out of business outright.

The past two years in particular have seen automation and AI (though some might question how many 'AI-enabled' solutions make use of 'true' artificial intelligence) heralded as at least a partial answer to these issues. They're seen as a way of addressing not just the growing variety and sophistication of threats, but also the need to maintain such a wide range of solutions, and the difficulty of hiring and retaining enough cybersecurity staff.

But while automation has a lot to offer, there's no such thing as a silver bullet solution. Neither a fully pared-down, 'eggs in one basket' solution or a precarious Jenga tower of tools is sustainable. Technological solutions are in most cases critical to an effective security posture, but they can't bear the full weight of a company's security, and they have to be chosen carefully based on the organisation's specific requirements, priorities and the threats it faces.

Our hope is that if nothing else, this collection of recommendations from in-house cybersecurity teams will help to simplify that process somewhat.