SPECIAL REPORT

WHO SECURES THE UAE?

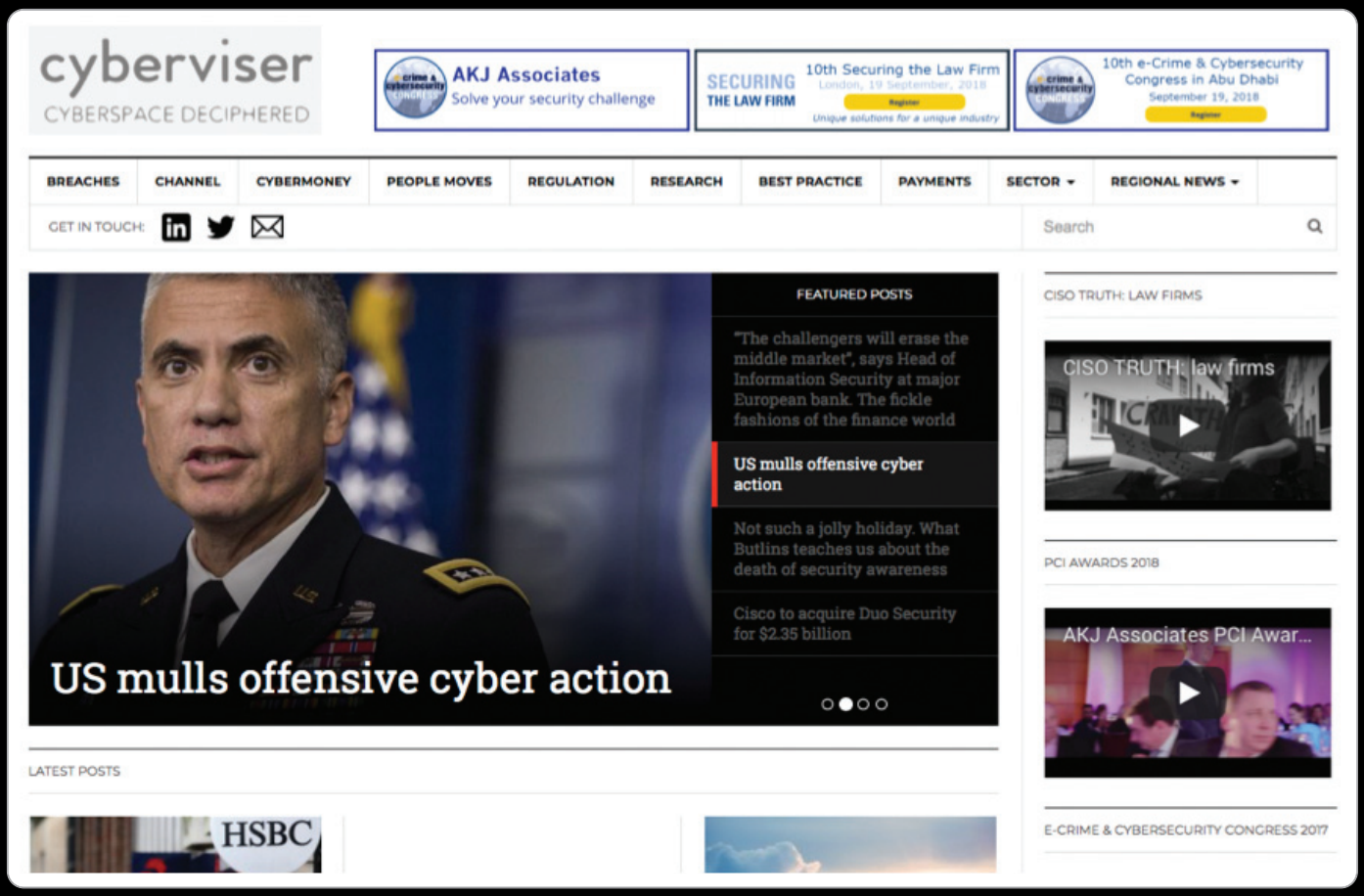
AKJ Associates

www.cyberviser.com – launching now!

You know AKJ Associates for its 20-year record of market-leading conferences and events in cybersecurity and compliance. Under the e-Crime Congress, Securing the Law Firm and PCI London brands, we have consistently tried to get ahead of the trends shaping your market and careers, instead of rehashing the same old ideas.

We were first to bring CFOs and institutional investors to you, to reveal what business and stakeholders really think about cyber. We were at the forefront of understanding the collision of cybersecurity, operational risk and compliance. And we have not been afraid to confront cybersecurity's many inconvenient truths.

To expand the resources we provide to you, we are launching a website to continue our mission of delivering independent thought leadership, news and views.



www.cyberviser.com will bring you:

- ✓ **Research and data:** AKJ Associates' proprietary data and conclusions gathered from security professionals around the globe. Our first project, 'Who Secures the UAE' is now live.
- ✓ **News and comment:** the most significant news stories with interpretation and comment from AKJ editors and the market.
- ✓ **Best practice:** what works and what doesn't, direct from leading end-users and security practitioners.
- ✓ **Regulation:** the latest global news on regulation and compliance, cross-sector, cross-region.
- ✓ **People:** who is firing, who is hiring and what are they paying? CISO profiles and interviews.
- ✓ **Vendors:** start-ups, funding, M&A, new solutions and new technologies.

SPECIAL REPORT

WHO SECURES THE UAE?

CONTENTS

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

CONTRIBUTING EDITOR
Amanda Oon
e: amanda.oon@akjassociates.com
t: +44 (0) 207 242 7498

EXECUTIVE SUMMARY

Over the past year, AKJ Associates has completed an extensive research project into the challenges facing CISOs in the UAE, and their thoughts on the solutions available.

To create a balanced, representative and truly relevant image of the landscape, we combined responses from over 150 of the region's information security professionals, representing a range of organisations, company sizes, and industries. Their responses were supplemented by further in-depth interviews.

Our research uncovered a number of interesting trends, key among them being the crucial importance of investment in staff resources.

According to our respondents, information security teams are understaffed in even the biggest companies. 35% of participants said that their organisation's information security team had two or fewer participants. Even at companies with over 5000 employees, fewer than half had information security teams of more than 5 members.

Other key findings include:

- Only 1 in 4 participants said that the CISO's knowledge of operational risk was fully appreciated by the board. This means that implementing real strategic changes and a truly mature security posture is likely to be a difficult process.
- Almost a third of participants said that they do not have as much board support as they need to effectively safeguard their company's critical assets.
- Information security professionals are generally positive about solution providers, with only 2% reporting a negative opinion
- The top problems end-users do have with solution providers are high prices (which is most likely related to the lack of board support), and the difficulty of differentiating between vendors in the crowded marketplace.
- Information security professionals are split almost exactly 50:50 on the subject of MSSPs, with a very slight majority saying they would not prefer to use one.
- Cisco was voted the best fit for participants' priorities in a provider, and was the most mentioned for effectiveness across a variety of risk areas.
- Information security professionals were least confident in the availability of adequate solutions when it came to 'Internet of Things' security and mobile device security.

2018 has already seen huge shifts in information security, with new technologies such as AI and blockchain becoming increasingly relevant, and new regulation such as the GDPR impacting data protection requirements around the world, not just in Europe.

As KS Ramakrishnan, Chief Risk Officer of Ras Al-Khaimah-based RAK Bank, says: "There's the continuing digitalisation of the economy. Obviously this means that there will be greater cyber development – and a lot more room for security vendors. But the risks will be a lot more profound – and I mean internationally ... now it is not really a matter of if but when. With the push to go digital in the UAE, there will be demand for security solutions."

As cybersecurity becomes more and more critical to the business, companies worldwide will need to increase their investment – not just in terms of budget, but taking into account hiring and company-wide strategic commitment as well.

Unless they do, the difficulty of defending against malicious actors may soon exceed the abilities of understaffed and underfunded information security teams.

INTRODUCTION

The past year has been an exciting one in the world of cybersecurity. When we began our project, the impact of WannaCry and NotPetya was still being felt worldwide - though the UAE wasn't hit as hard as Europe, the media attention brought the real business impact of cybersecurity to the attention of senior management. AP Moller-Maersk's NotPetya damages were estimated at up to $300 million, and the breach at Equifax – often considered the worst corporate data breach to date – cost the company $439 million.

Since then – thanks particularly to the introduction of mandatory disclosure in Europe – a vast number of high-profile breaches have made the headlines. Breaches in the UAE, which more often go unreported, have also come to light, with Dubai-based Careem reporting a breach which affected more than 14 million users' data in April.

These incidents and many others like them have brought information and network security into the limelight as a real business concern – but though there's been plenty of talk, what has changed? Every year we see headlines announcing dramatic new developments and record-breaking incidents in the world of cybercrime, [1] and unless something changes drastically, we will see similar headlines for years to come. In part that's down to the nature of reporting, but what is clear from this is that if new innovations and levels of effectiveness from hackers are an inevitability, we need to limit the damage a potential breach is able to do.

While company-wide security awareness training is one way of mitigating these risks, it can take just one wrong click to jeopardise an entire system. We cannot rely on each employee never making a mistake, no matter how well-trained or well-intentioned they are, especially considering the shortage in the cybersecurity workforce. Accordingly, an effective security infrastructure which can minimise the threat posed by slip-ups is vital.

Vendor ecosystem too complex

Unfortunately, that comes with complications of its own. The complex and fragmented nature of the vendor ecosystem – particularly in regions where many vendors do not have a local presence and sell exclusively through resellers – makes the theoretically simple task of buying and implementing the appropriate solutions a daunting challenge. The growing coverage of cyber-attacks in mainstream media, and increasing board-level appreciation of the real financial and business risk of a successful attack, may have resulted in increased spending power for some cybersecurity professionals,[2] but even so budget is not unlimited. Even if it were, the procurement process is not as simple as just putting money into a solution and getting an equivalent amount of security out: different solutions are appropriate for different business requirements, and are varyingly effective.

"You need to have business priorities in mind...starting out you always have to think about costing. Cost optimisation. There is a risk budget. You need to think about your requirements...you always need to be forecasting. There is a lot of variety of software on the market. You have to choose the best one for you," says Noura Al Qubaisi, CISO, ADMCC.

---

1 Bloomberg, '2016 Was A Record Year For Data Breaches', Digital Guardian, '2015 Midyear Review: The Biggest Data Breaches Year To Date', The Telegraph, 'The biggest ever cyber attacks and security breaches', HelpNet Security, '800M exposed records make 2013 record year for data breaches', and Enterprise Innovation, 'Record data breaches in 2012', to pick just a few examples.
2 Gartner predicts that worldwide information security spending will reach $124 billion in 2019, with senior analyst Sam Olyaei predicting growth percentage in the double digits in the MENA region.

As procurement decisions are often just one of the many responsibilities an individual or team has to deal with, the process – when carried out with the diligence it deserves – is far more intensive in terms of time and labour than it needs to be.

Much of the information that is readily available about security products is marketing put out by the vendor company itself, and it is 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 them the whole story about a product's capabilities.[3] Furthermore, even moving past the shortlisting stage and experiencing services first-hand is not necessarily reliable: multiple participants in our research told us that they do not consider a proof of concept to reliably indicate the level of support a vendor will provide after the money has changed hands.

More than 17% of participants in our survey said they were using more than 10 distinct solutions in their cybersecurity stack, and supplementary interviews indicated that this was considered necessary not just because of complex security requirements, but to cover for flaws in other solutions.

Cybersecurity professionals simply do not have the resources to continue trying solution after solution in the hopes of finding the best ones for their needs, and the amount of time and energy (let alone money) spent on compensating for inefficiencies in commercially licensed software keeps an already overworked team from focusing on other responsibilities.

End-user research critical

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 more casual environment, are key to understanding the relevance of the available solutions.

But outside of specially organised networking events with strict policies on confidentiality, people may worry about the potential risks of openly discussing weaknesses in the products they use. Turning to consulting firms is one possible remedy, but can you rely on them for unbiased advice?

To help address these concerns, we have carried 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 providers they have found most effective in addressing their specific requirements. While no substitute for the level of pertinent and in-depth insight provided by direct peer-to-peer discussion, we hope it will nonetheless be a valuable resource.

---

3 E.g. Gartner, 'How to Tell When Vendors Are Hyping AI Capabilities', Channel Web, 'Security vendors are 'mis-selling technology – security reseller'.

THE CHALLENGES FACING THE UAE

Despite the UAE's relatively small population, its IT industry is booming. A Geneva Papers report showed that digital markets in the Middle East are expanding at an annual compound growth rate of 12%,[4] and a report published by McKinsey ranked the UAE government number one in digital adoption among Middle Eastern countries, with advancements spreading 'at an accelerating speed'.[5]

The UAE stands out worldwide, too. IMD's 2018 Digital Competitiveness Report, which ranks countries by their ability to adopt and adapt digital technologies, ranked the UAE 17th globally and 10th in the EMEA region. [6] It was also ranked first globally for business agility, second for cybersecurity, fourth for talent, and seventh for technology.

"Being top class Gartner is all very well. But if all we're going to get is an expensive solution that won't be fit for purpose then there's no point," KS Ramakrishnan, CRO, RAK Bank

This is reflected by projects such as the Smart Dubai and Abu Dhabi initiatives, which clearly show the commitment to the role of new technological advancements in the region's development.

However, rapid growth brings with it a variety of potential threats, which need to be considered not just by IT professionals but also by other board-level executives and by security product vendors looking to operate in the region.

One of the points raised by participants in the survey we sent out, and in the supplementary interviews we conducted, was that many of the solutions provided by vendors simply do not take region-specific issues into account. Solutions and business models that work elsewhere might need adjustment in order to be fully effective in the UAE, and the feedback we have received is that many international vendor companies seem not to accomplish this.

"When you decide to implement something, it can be a challenge. Not everything is suitable in this part of the world, which means you have to be cautious with the execution phase as the selection of the partner is a key success factor in any project. It's not all about the solution, it's a mix between the solution and the partners the vendors have locally," explains Antonio Dionisio, CISO, MIG Holdings.

Lack of local support from vendors

Many international vendor companies do not have a strong on-the-ground presence in the UAE, and instead use local resellers to distribute their products. Due to the relatively small size of the UAE, large international companies may question whether they need to commit their resources to establishing a local presence.

In many cases, product support provided through resellers will be supplied by representatives

4 Geneva Papers, 'Cybersecurity Challenges in the Middle East'
5 McKinsey, 'Digital Middle East'
6 IMD, 'World Digital Competitiveness Ranking 2018'

with responsibility for multiple products. This has its advantages: knowledge of a range of security solutions means that resellers can help customers make the best decisions, and at least in theory these representatives are unbiased.

However, resellers are still running a for-profit business, and in reality their commission on a sale is likely to factor into their recommendations. Additionally, multiple participants in our research have commented on negative experiences they have had with resellers whose knowledge of a specific product has been inadequate.

Even in cases where the reseller is doing everything right, the greater difficulty of directly accessing the original vendor company can be a problem, and while local resellers should be able to advise on region-specific issues, the vendor company itself may be unaware of these issues and therefore unable to take them into account.

"We of course work with some vendors who do not have a local presence. But local knowledge is important. We look for things like is there support available at our timings? And do you know the market? Otherwise there's no point. Even if there's no physical presence, you have to know our market," says KS Ramakrishnan, CRO, RAK Bank.

Insufficient training and awareness

Rapid growth in any sector requires a solid foundation in terms of infrastructure and human resources to support it. There is a shortage of skilled IT professionals worldwide, and this particularly affects the UAE.[7]

Though IMD's report rates the UAE fourth globally for talent, the 2016 Hays Salary & Employment report noted that many IT professionals from GCC countries have been attracted away to the USA, the UK and Asia;[8] combined with the UAE's relatively small population and its high staff turnover rate, it is easy to see why its IT workforce might struggle with the constant push for transformation.[9]

"Employers and government sponsors are prepared to invest in building local talent, including travel if that is required to produce better learning outcomes," Sebastian Madden, CEO, PGI

This is a particular concern given the speed of adoption of newer technologies, especially for business use, which may have additional security needs that IT professionals need to keep on top of.

A key requirement in these circumstances is a vastly increased training and education infrastructure not simply to create the next generation of cybersecurity professionals from the ground up, but also to upskill current employees.

PwC recently reported that one of the key risks facing security in the Middle East is the

7 The worldwide IT skills shortage is discussed in Kaspersky's 2016 IT Security Risks report, which found that almost half of the 4,000 business representatives interviewed worldwide felt that more specialists in IT security were needed, and McAfee's 2016 Hacking the Skills Shortage report, in which over 80% of respondents reported a shortage of cybersecurity skills. In specific regards to the Middle East and particularly the UAE, only 35% of participants in the 2017 ACN IT Salary Survey reported that their IT teams were fully staffed.

8 Hays, 'Salary & Employment Report 2016'.

9 Gulf News, 'Staff turnover in the UAE higher than global average'; in terms of the IT sector in particular, the ACN IT Salary Survey found that only 17% of participants were not interested in changing jobs over the next six months.

tendency to buy "a technological 'fix'" for cybersecurity issues rather than investing adequately in training.[10] This is reflected in the IMD report, which despite rating the UAE 4th for talent, puts it 56th globally for training and education.[11]

That said, there are vendors providing training to UAE firms and they find local firms prepared to invest, and even to travel to the UK for upskilling: "Our training programmes typically take people from one level of cyber security competence to the next using short courses. That doesn't normally require a "resident trainer". We can either fly our UK-based trainers out to the region with mobile training infrastructure or remote connections back to our Academy infrastructure or the delegates come back to the Academy in the UK to train. Delegates are usually very happy to come to the UK for training. Employers and government sponsors are prepared to invest in building local talent, including travel if that is required to produce better learning outcomes." says Sebastian Madden, CEO, PGI.

Network Middle East's study found that less than half of their participants' organisations had an ongoing security awareness campaign, and 19% said their organisation had no security policy at all.[12] Though underinvestment in training is a global issue – an article by Symantec comments on organisations 'incorrectly equating bigger investments in security technology and services with adequate coverage'[13] – it is particularly difficult to combat when combined with a limited workforce, particularly one with high turnover rates.

SANS recommends that to bring security standards among non-IT employees up to even a basic level, organisations should have on average 1.4 full time employees dedicated solely to security awareness initiatives, and 2.6 if more than a basic level of awareness is desired.[14]

Among our participants, the most common size for an entire information security team is 1-2 members. Without increased hiring – problematic, given the already limited workforce – effective training programs will be difficult to put in place without enlisting outside help.

A report found that 57% of UAE companies surveyed considered staff the weakest point in their security, but that only 39% were looking to address this by investing in training.[15] The consequences are demonstrated by a recent incident in which CCTV cameras in Dubai homes and places of employment were found to be broadcasting live footage, which was attributed to installation by technicians who were "ignorant about their job and lacked experience".[16]

Attackers prey on this ignorance and lack of experience to get around technological defences: 26% of targeted attacks on UAE businesses in 2016 - 2017 revolved around phishing or social engineering, and 46% of IT security incidents around the world were caused by employees.[17]

The lack of investment in training also applies to IT professionals, with 54% of participants in a recent survey reporting that they had received no on-the-job training – worrying, in a sector where change happens at such a rapid pace.[18]

---

10 PwC, 'A false sense of security? Cybersecurity in the Middle East'.
11 IMD, 'IMD World Digital Competitiveness Ranking 2018'.
12 ITP, 'The year in threats: NME 2017 Security Survey'.
13 Symantec, 'Is Your Firm Resting on its Security Laurels?'.
14 SANS, '2017 Security Awareness Report'.
15 Tahawul Tech, 'UAE employees conceal most IT security incidents: study'.
16 Gulf News, 'Hackers found broadcasting CCTV footage from Dubai homes'.
17 Tahawul Tech, 'UAE employees conceal most IT security incidents: study'.
18 ITP, 'A positive outlook: ACN IT Salary Survey 2017'.

Deliberate targeting by criminals

Areas of rapid growth and development are often seen as a soft target by criminals, and the UAE, as one of the wealthiest countries per capita and a major player in the oil and gas industries, is a very tempting target. While IMD rated the UAE 17th globally in terms of digital competitiveness, a 2015 report by Kaspersky Labs ranked it 19th in terms of vulnerability to online infection.[19]

Though a more recent ranking is not available for direct comparison, Kaspersky's 2017 Cybersecurity Index shows that 42% of UAE residents have been affected by cybercrime, with 29% having been infected with a virus or malware, approximately 1.5 times the global figures of 27% and 18% respectively.[20] Telecom company Du found similar figures, reporting in 2016 that two in five Dubai residents have been victims of cybercrime.[21]

This disparity is simply not proportionate to the difference in online activity levels discussed above. Targeted attacks on UAE-based victims accounted for 5% of all global cyberattacks in 2016 and have increased by more than 500% over the last five years,[22] and a 2017 report by InfoWatch found that 70.6% of data leaks in the UAE are caused by external violators compared to 41.7% globally.[23]

Victims' losses have been considerable: a 2017 report by the Ponemon Institute found that the average total cost of a data breach in the UAE and Saudi Arabia that year was over 18,000,000 AED.[24] PwC found that Middle Eastern companies have suffered losses greater than the global average as a result of cyberattacks, with 85% having suffered an attack compared to a global average of 79%, and 56% of affected businesses having lost more than 500,000 USD (approximately 1,836,600 AED) compared to a global average of 33%.[25] These findings suggest that while the UAE is already disproportionately targeted by cyber criminals, the situation is only getting worse.

Difficulty of securing the internet of things

It's not only private citizens and businesses who are at risk: at the Arab Future Cities Summit in 2017 the president of InfoWatch, speaking in relation to smart city initiatives in GCC countries, expressed her concern that security systems "are not able to catch up effectively" with new technological developments.[26]

She is far from the only one worried by the apparent fact that new developments in terms of technology, particularly devices connected to the 'Internet of Things' (which plays a huge role in smart city infrastructure), are being developed and sold without adequate thought given to

19 Kaspersky, 'Kaspersky Lab reports UAE among the top-20 countries facing the greatest risk of online infection in 2015'.
20 Kaspersky, 'Kaspersky Cybersecurity Index'.
21 The National, 'Two in five are cyber crime victims'.
22 Gulf News, '5% of global cyber attacks targeted UAE last year'.
23 Infowatch, 'Data Leakage Report Q1-Q3 2017 Middle East'.
24 Ponemon, '2017 Cost of Data Breach Study: Middle East'.
25 PwC, 'A false sense of security? Cybersecurity in the Middle East'.
26 The National, 'Smart cities open door to cyber-attacks, say security experts'.

how they might be secured: a "build, ship and forget" model, as Irdeto's Mark Hearn calls it.[27]

The exploitation of seemingly harmless devices such as fish tanks and refrigerators for use against individuals and companies is a real risk, as we have already seen in various amusing and worrying headlines in recent years.[28]

However, even leaving aside the potential financial and reputational repercussions of breaches resulting from smart device hacking, these methods could in more dramatic scenarios be used to cause chaos, serious injury and even death.

One of the better-known examples from recent years is the demonstration of how a Jeep Cherokee could be remotely hacked,[29] and concerns have been rising about the 'Hollywood'-esque disasters that could arise were a malicious individual or group to gain access to traffic light systems, electricity grids or power plant controls.[30] This threat is not exclusive to the UAE, but it is certainly one that stands out as prevalent in this region, and it has grown enormously during the past few years.[31]

So how do we address those threats?

These are the challenges the IT workforce in the UAE is facing. They can be broken down into two major issues. First, rapid technological advancement in the region is outpacing the average employee's level of training and awareness, and requires more time and resources than overwhelmed IT professionals are able to provide without making compromises. Second, criminals are recognising these vulnerabilities and applying even more pressure by deliberately targeting UAE businesses, which they see as relatively soft targets.

Ideally, security software should be helping by automatically handling the majority of the threats IT and information security professionals have to deal with, thus allowing them to work on addressing the more structural challenges we've discussed here. However, the viability of security software as a real solution depends heavily on the cost – in terms of time as well as money – of purchasing, deploying, finetuning and maintaining it.

Even in organisations with enough resources that this is not a major concern, the amount of time taken to achieve optimal effectiveness will have operational repercussions.

For the majority of professionals in cybersecurity and related fields to be able to seriously combat threats rather than simply reacting to them, the process of choosing and

---

27 Irdeto, 'New IoT Security Bill is One Step Toward Fixing a Global Security Problem'. The threat posed by IoT devices, particularly in the Middle East, is also discussed in a variety of other articles, e.g. Tahawul Tech, 'Poor cybersecurity hygiene, risky apps enable destructive attacks', NES, 'NES emphasizes critical importance of Smart Grid security', Forbes, 'Internet of Things By The Numbers: Market Estimates and Forecasts'.

28 Washington Post, 'How a fish tank helped hack a casino', The Guardian, 'CloudPets stuffed toys leak details of half a million users', BBC News, 'Fridge sends spam emails as attack hits smart gadgets'.

29 Kaspersky, 'Shock at the wheel: your Jeep can be hacked while driving down the road'

30 SecureRF, 'IoT Security Vulnerabilities of Smart Cities', Harvard Business Review, 'Smart Cities Are Going to Be a Security Nightmare'.

31 For example, in a study on the topic, Kaspersky detected 46 samples of malware for IoT devices in 2013, a figure which has grown exponentially each year since, with an article published in June 2017 reporting 7242 samples found so far that year. They also reported that since the start of 2017 they had detected over 2,000,000 hacking attempts targeting IoT devices, and more than 11,000 unique IP addresses from which IoT malware was downloaded (Kaspersky, 'Honeypots and the Internet of Things').

implementing the most effective solutions needs to become far less convoluted.

Spending months just on finding out whether products meet your needs, to say nothing of the risks of purchasing a solution and then discovering it is not fit for purpose, is simply not an option in the current threat environment.

There needs to be a quicker, easier and more reliable method of finding out what the best solutions will be for your company's specific needs. We believe that information-sharing is that method.

That's why we've spent the last few months putting together this report, which compiles insights from the Middle East's top IT and information security professionals, covering a wide variety of industries, business sizes, and security priorities. This information will help end-users to evaluate not simply whether a solution works, but whether it will work for them.

WHO PARTICIPATED

Our primary source of information in compiling this report has been a questionnaire which we sent out to attendees at our events in the UAE, as well as to a selection of new contacts picked to ensure a more representative sample.

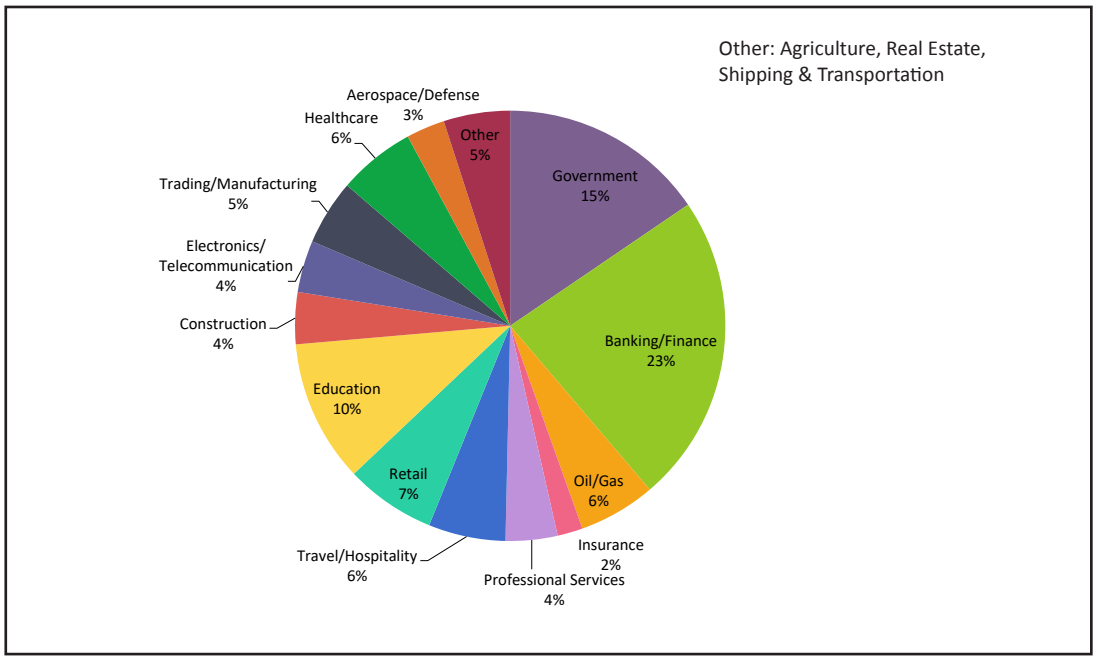
This questionnaire consisted of 23 questions, some of which were to establish demographics (for example questions about industry and company size), but most of which concerned participants' feelings about and experiences with the security solutions market.

The survey was anonymous, but personalised links were sent out to the potential participants so that each individual was only able to complete the survey once. Information obtained in this way was then supplemented by more in-depth discussions with selected individuals.

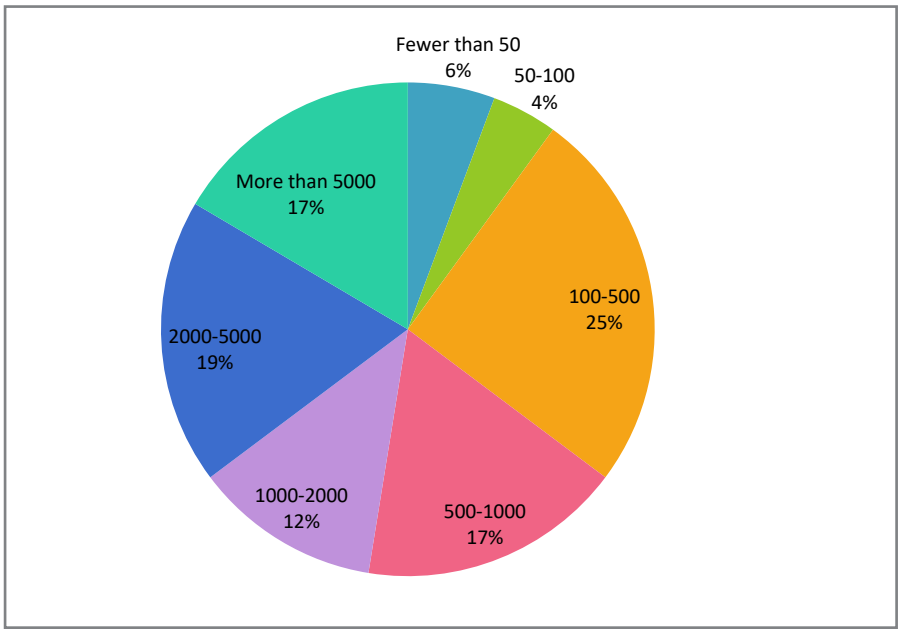
We received over 150 responses, primarily from individuals whose company or branch is based in the UAE. All participants were individuals who deal with IT security and infrastructure, whether in a direct decision-making capacity or otherwise, and represent a number of organisations in different industries, including major banks, national government, and high-profile retail operations.

The demographic make-up of survey participants is demonstrated in the following charts, in which all percentages are rounded to the nearest whole number:

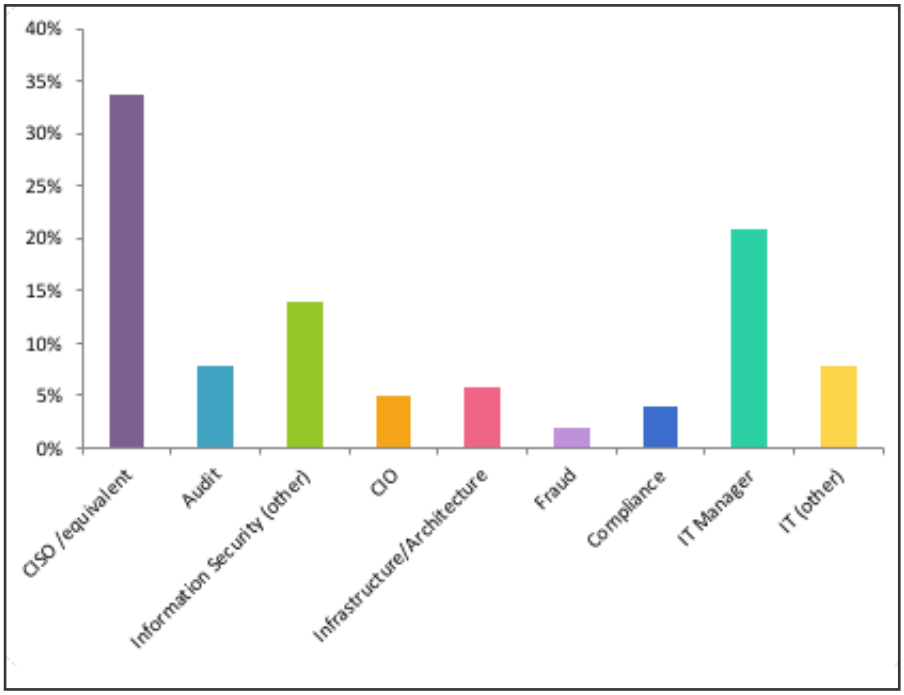
INDUSTRY



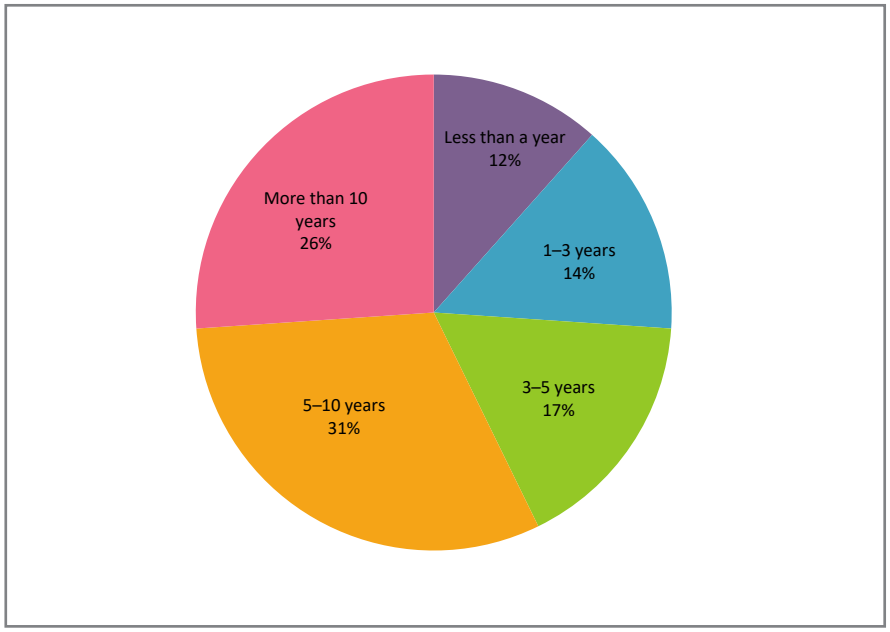
SIZE OF COMPANY (BY NUMBER OF EMPLOYEES)



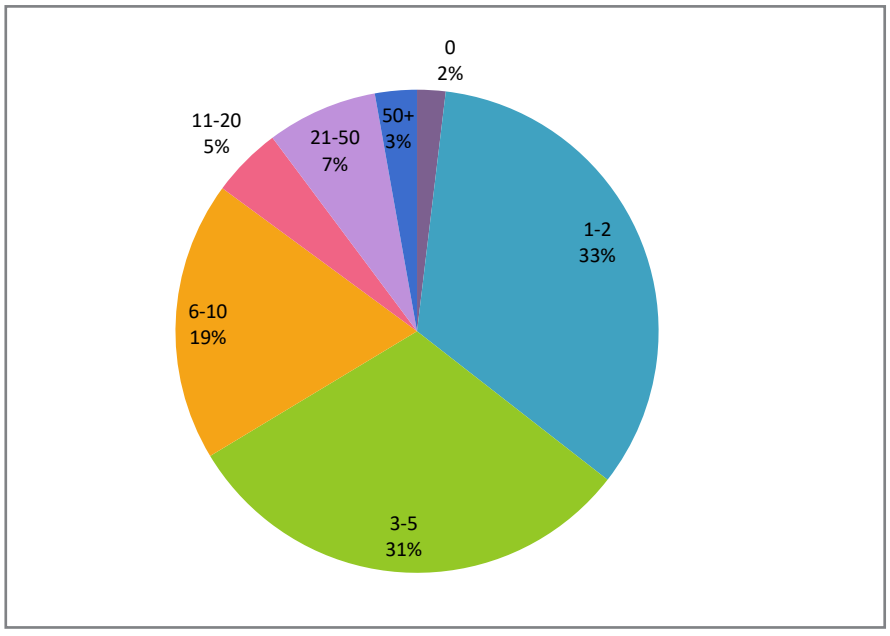
ROLE IN COMPANY



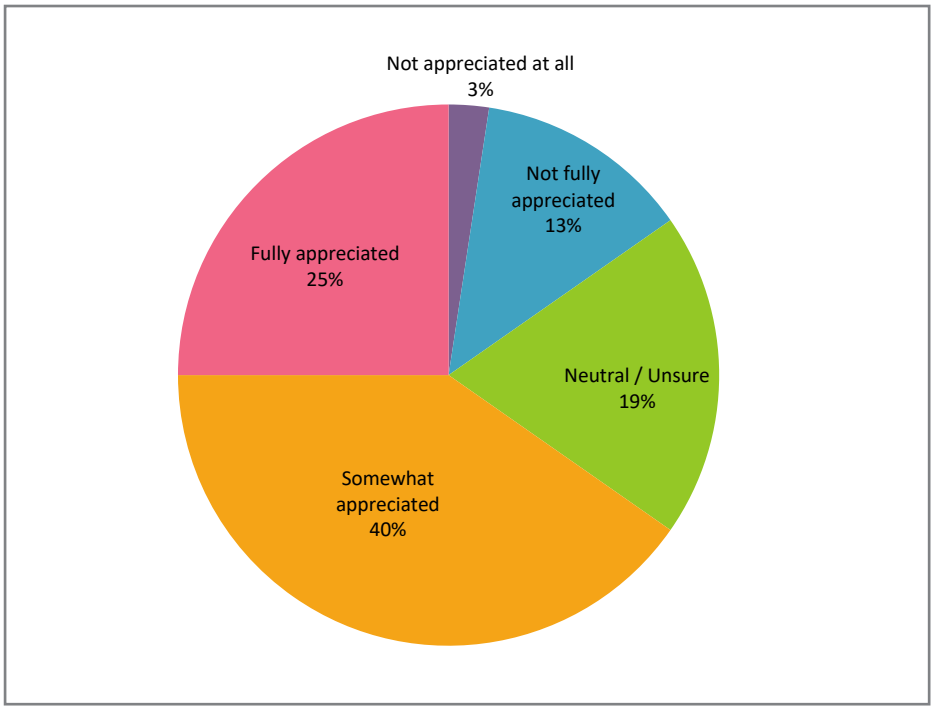
YEARS' EXPERIENCE IN CYBERSECURITY



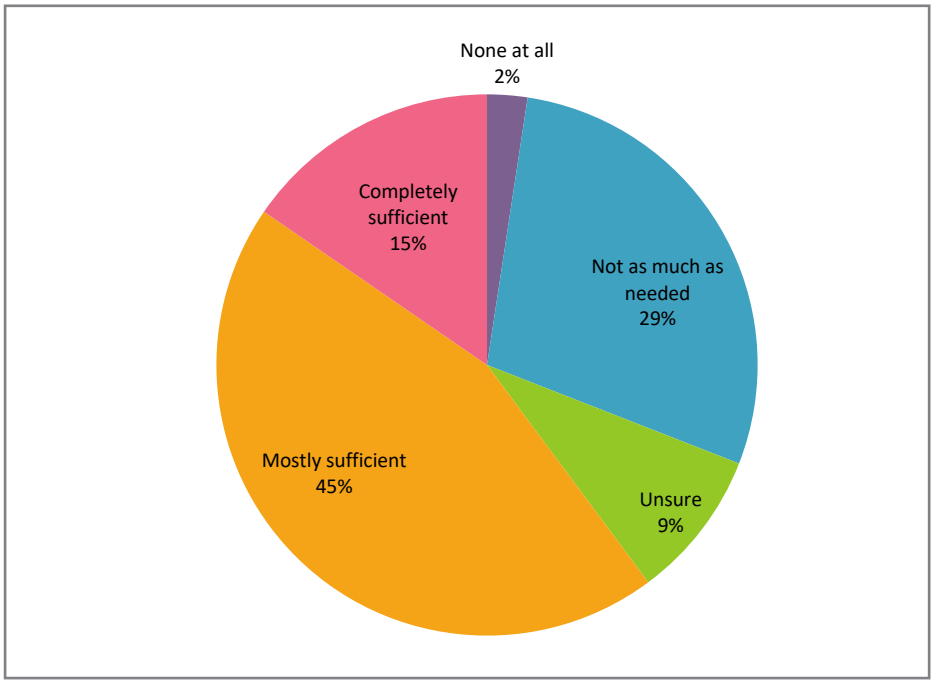
NUMBER OF EMPLOYEES IN INFORMATION SECURITY TEAM



PERCEIVED LEVEL OF BOARD APPRECIATION FOR CISOS' KNOWLEDGE OF OPERATIONAL RISK



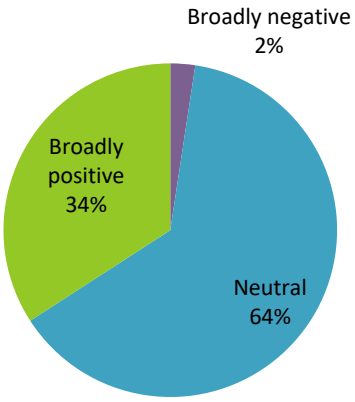
PERCEIVED LEVEL OF BOARD SUPPORT



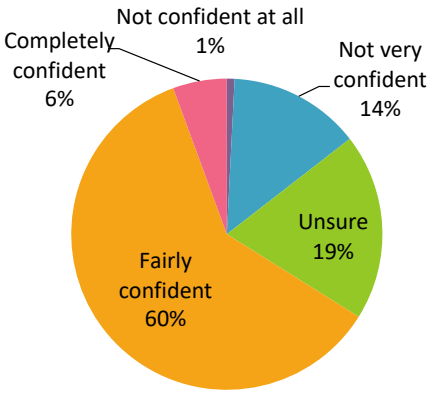
FINDINGS

One of the primary areas our research has looked at is how end-users feel about the marketplace for security solutions, and where they think improvements need to be made:

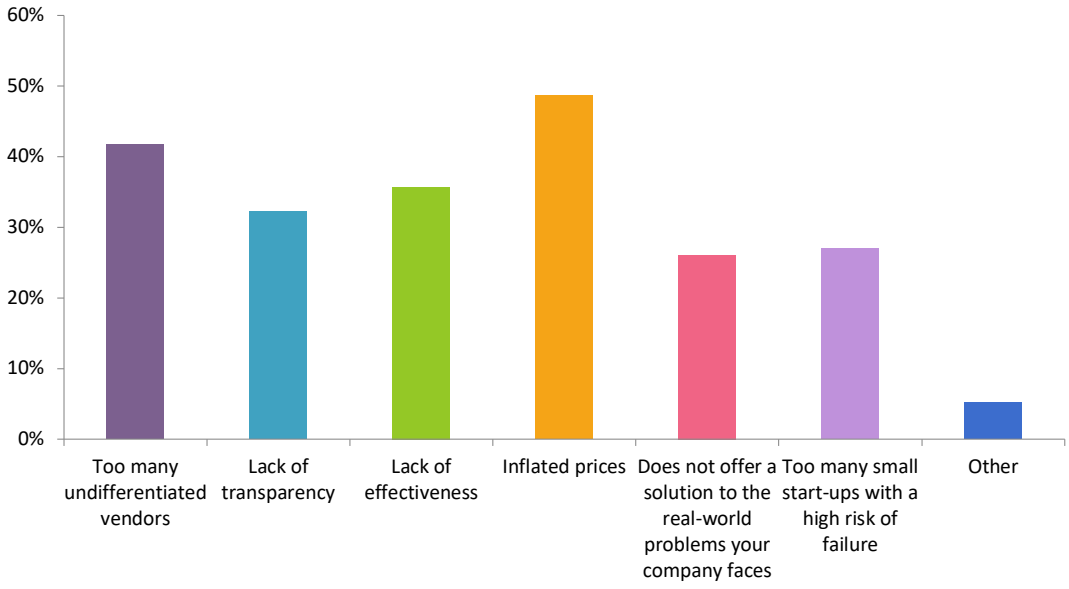
OVERALL IMPRESSION OF THE CYBERSECURITY VENDOR ECOSYSTEM



CONFIDENCE IN RELIABILITY OF INFORMATION EASILY AVAILABLE ABOUT SOLUTIONS

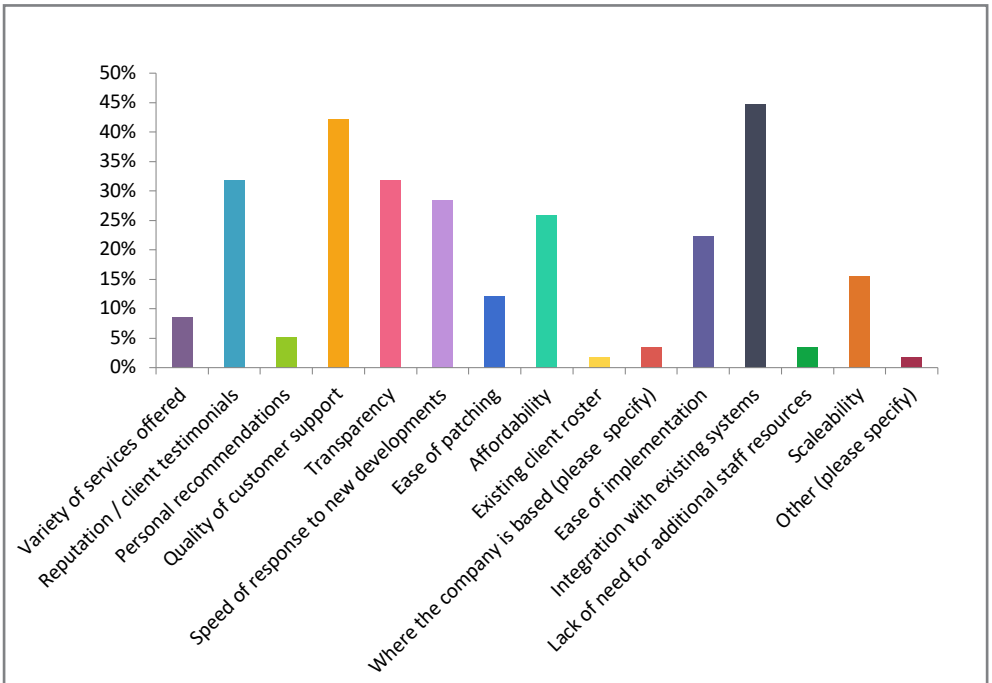


PERCEIVED PROBLEMS WITH VENDOR MARKET



**Other: Lack of specificity or relevance to the region was the response given most frequently, with "N/A" as the second most frequent, presumably meaning that these participants did not believe there were any problems with the vendor market. The other criticism mentioned in this field was 'inflated proposals'. One participant also reported, in the 'additional comments' field at the end of the survey, having dealt with a vendor company whose project management and implementation teams did not have "any knowledge" about the product – though interestingly, this participant did not report any concerns about transparency or the reliability of information.*

TOP THREE PRIORITIES IN A SOLUTION OR SOLUTION PROVIDER



**Where the company is based: All UAE, with some votes specifying Abu Dhabi or Dubai*
***Other: Responses entered here referred to "business-oriented knowledge" and to an understanding of industry-specific threats.*

These results show a mostly positive perception of the solutions market, though over a quarter of participants did not report feeling confident in the reliability of the information easily accessible to them. In terms of priorities, the high importance placed on 'quality of customer support' is predictable as a result of the limited information security workforce, and the low number of locally-based direct vendor representatives.

Likewise, the number of votes for 'integration with existing systems' is unsurprising, given the number of participants who told us that they were working with complex multi-vendor security architecture.

"One of the reasons we've grown so fast is that we work with other vendors! Our platform is open. Because our mission is to prevent successful cyber-attacks and our main enemy is the cyber-criminals, our goal is partnership. We all really have to work together – any vendor in the industry can put their solution on our platform. It doesn't matter if it's our licence or someone else's. And we have grown 31% which tells you something about whether that is a good strategy," says Ercan Aydin, Director, Emerging Markets, Palo Alto Networks.

The fact that 'reputation/client testimonials' and 'transparency' are ranked third and fourth respectively likely reflects concerns about the reliability of the information available about solutions – and the importance of making the right decisions.

The low number of votes for 'existing client roster' and 'lack of need for additional staff resources' is somewhat unexpected, as these are concerns which were raised to us in direct

Closing the cyber skills gap by reskilling workforces

Sebastian Madden, Chief Corporate Development Officer
Protection Group International

It's tough trying to staff your organisation to manage its cyber security risks. Good cyber professionals are hard to find, expensive to hire, and quickly move on to new jobs. This is because of the "cyber gap." This is the difference between the demand for cybersecurity professionals and their supply. It is projected to reach 1.8 million by 2022, making professionals hard to find. This is compounded by hiring managers preferring to recruit based on experience, luring staff from other organisations with better pay.

This model is unsustainable. It drives up salaries and raises the cost of security. It is also risky. Not all the expensive, experienced professionals are any good. And even those that are may take time to get up to speed in a new company, or sector. A survey for the UK financial services sector found it can take up to four years for a new security professional to fully understand the complex and bespoke infrastructure of a major bank. Similar challenges face those joining critical national infrastructure providers.

"Second is a partnership with forward-thinking government agencies or employers who are looking to create or hire cyber security professionals"

Reskilling programmes – where people with aptitude are quickly trained in the basics of cybersecurity to perform frontline roles – are therefore becoming an increasingly popular option. In the last 12 months, the specialist UK cybersecurity consultancy and training company, PGI has been involved in several pioneering reskilling programmes in Europe and the Gulf region, which were established to tackle specific aspects of the cyber skills shortage. These have used PGI's state-of-the-art Cyber Academy and training expertise to equip people from a variety of countries and backgrounds with the skills, experience and certifications. This has allowed them to move seamlessly into the cybersecurity profession where they are badly needed.

Programmes that PGI has supported have included:

- The UK and Saudi phases of a six-month programme 'Secure17'. This was for nineteen Fellows selected from several thousand applicants, sponsored by the Saudi Arabian Monetary Authority (SAMA) and run by Saudi cybersecurity specialists Trusted Security Inc. Abdulrahman Bajaber, Managing Director of Trusted Security Inc, describes the programme as "a one of a kind programme to equip Saudi youth with solid cybersecurity knowledge, skills and experience."
- The Kuwait Cyber Security Leaders Programme: a six-month programme sponsored by the Central Bank of Kuwait and run by the Kuwait Institute of Banking Studies. This was designed to retrain Kuwaiti nationals with strong IT skills and experience to become senior information security professionals within the banking sector;
- A three-month training programme in the UK with Hawker Chase, sponsored by the world's leading independent, end-to-end IT services and solutions company to retrain former Armed Forces officers with little or no background in cybersecurity to fill vacant roles in its cybersecurity teams; and
- Women in Cyber: A three-month UK government sponsored training programme to address diversity issues in the cybersecurity profession by training women who are looking to start a different career to perform entry level professional cybersecurity roles and guaranteeing them jobs before training starts.

According to Brian Lord, the Managing Director of PGI Cyber, the recipe for success in such programmes is relatively straightforward. "Aside from quality training that is technology agnostic and focused on the skills needed for specific, sought-after roles, a successful reskilling programme will have three main features. First is a selection process that ignores a candidate's cybersecurity or even technical background. It gauges their aptitude for technical or non-technical cybersecurity roles and allows the training to do the rest. Second is a partnership with forward-thinking government agencies or employers who are looking to create or hire cybersecurity professionals. They realise that existing cybersecurity experience is not a pre-requisite for all roles and are prepared to offer jobs and opportunities to successful alumni. Finally, an assessment and interview process that allocates candidates to streams within the

cybersecurity profession on the basis of early results so they can focus their studies. Ideally, this will include interviews with future employers that result in job offers and specific roles for the candidates to focus on during the rest of the programme."

Although typically staff with no technical background move into Information Security policy, GRC or SOC Analyst roles, these programmes have also found hidden technical talents with individuals from non-technical backgrounds being successfully certified for technical roles. On one recent programme, a delegate from a non-technical background finished top of the class in PGI's technically demanding GCHQ Certified Security Operations Centre Incident Responder course. As one recent graduate, former Army Captain Joe Chmiel, put it: "I've gone from having no technical experience of note, to holding a wide range of qualifications from numerous vendors and in a range of disciplines, including digital forensics, penetration testing, incident response, SOC analysis and information security management."

By opening opportunities in cybersecurity to staff from non-cyber security and even non-technical backgrounds, reskilling programmes benefit employers as well as employees. For Brian Lord "these programmes get more and more people into the profession. This starts rebalancing salary levels that are currently out of control, making the cost of cybersecurity more affordable. And by reskilling staff who already work for your company, you can harness their experience of other elements to inform your cyber security approach and policies. Existing staff know your clients, sector, culture, business drivers, as well as – in the case of your IT staff – your IT and operational systems and networks that they have built, operated, supported, and maintained, in ways external hires will inevitably take time to develop."

The outstanding results of these programmes – with alumni now successfully working in full time employment as Information Security Specialists; Governance, Regulation and Compliance (GRC) officers; SOC analysts; and Penetration Testers – show that it is more than possible to take individuals with little or no previous cyber security experience and quickly reskill them to the point where they can be certified to perform full-time, frontline cybersecurity jobs well.

Programme sponsors are seeing the results they were looking for too. In Saudi Arabia, according to Abdulrahman Bajaber: "the result of Secure17 was fascinating. 100% of the Fellows have been selected

for work in five different government departments and five different banks. And SAMA has now kicked off Secure18 with an increased number of Fellows." And in the UK, all twenty veterans who attended the armed forces reskilling programme were successfully hired into full-time cyber security roles in the sponsoring IT company following interviews and aptitude tests; and engaged in their new jobs immediately after the programme ended. Simon Vaughan-Edwards, Managing Director of Hawker Chase, says "we are delighted with the success of this programme which has found individuals coming straight out of the armed forces wonderful jobs with a great employer and is solving some of the UK's cyber personnel problems." ■

Links

Secure17 results and announcement of Secure18
http://www.sama.gov.sa/en-US/News/Pages/news11072018.aspx

Kuwait Cyber Security Leaders Programme
http://www.cbk.gov.kw/en/cbk-news/announcements-and-press-releases/press-releases.jsp?kcp=o8QTtSFuP5Ix5WoYWwE74iHHgN8rIQ==

Arabic language introduction to Armed Forces Retraining programme story on PGI's Cybrani LinkedIn site
https://www.linkedin.com/feed/update/urn:li:activity:6433768647986020352/

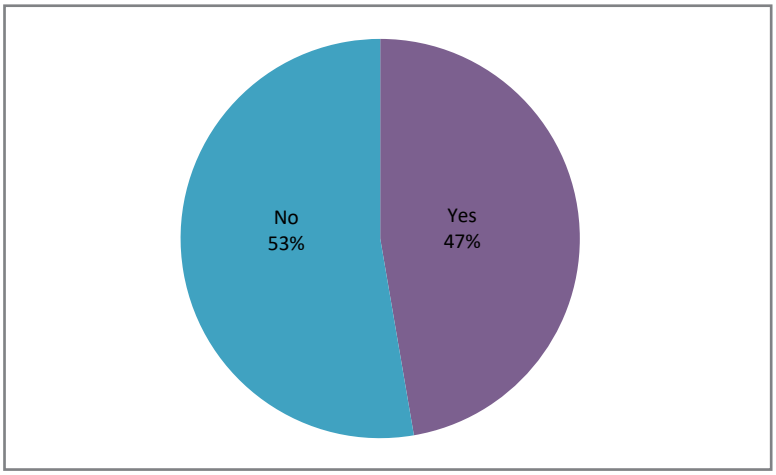
Armed forces retraining programme
https://www.ctp.org.uk/focus/job-finding-cyber-security-roles-with/488776

Joe Chmiel's storys
https://www.pgitl.com/explore/article/cyber-retraining-programme-armed-forces-to-cyber-conversion-joes-story

Women in Cyber
https://www.pgitl.com/training/programmes/women-in-cyber

conversation; however, the most likely explanation is that as participants in the survey were restricted to selecting three options, they may have felt that 'existing client roster' was covered under 'reputation/client testimonials', and that 'lack of need for additional staff resources' was covered under either 'affordability' or 'ease of implementation'.

Given that integration of solutions was such a high priority, we were curious as to how cybersecurity professionals felt about Managed Solution Service Providers, which we thought might be one way of ensuring successful integration while significantly cutting the time spent on procurement decisions and on monitoring multiple programs. The overall vote on whether participants would prefer to use an MSSP shows a fairly even split:



Although the numbers are close, we received multiple comments on the disadvantages of MSSPs from our participants.

The main points raised were the danger of a vulnerability being discovered in the MSSP, data protection issues (particularly with companies based outside the UAE), and lack of 'best-of-breed' quality.

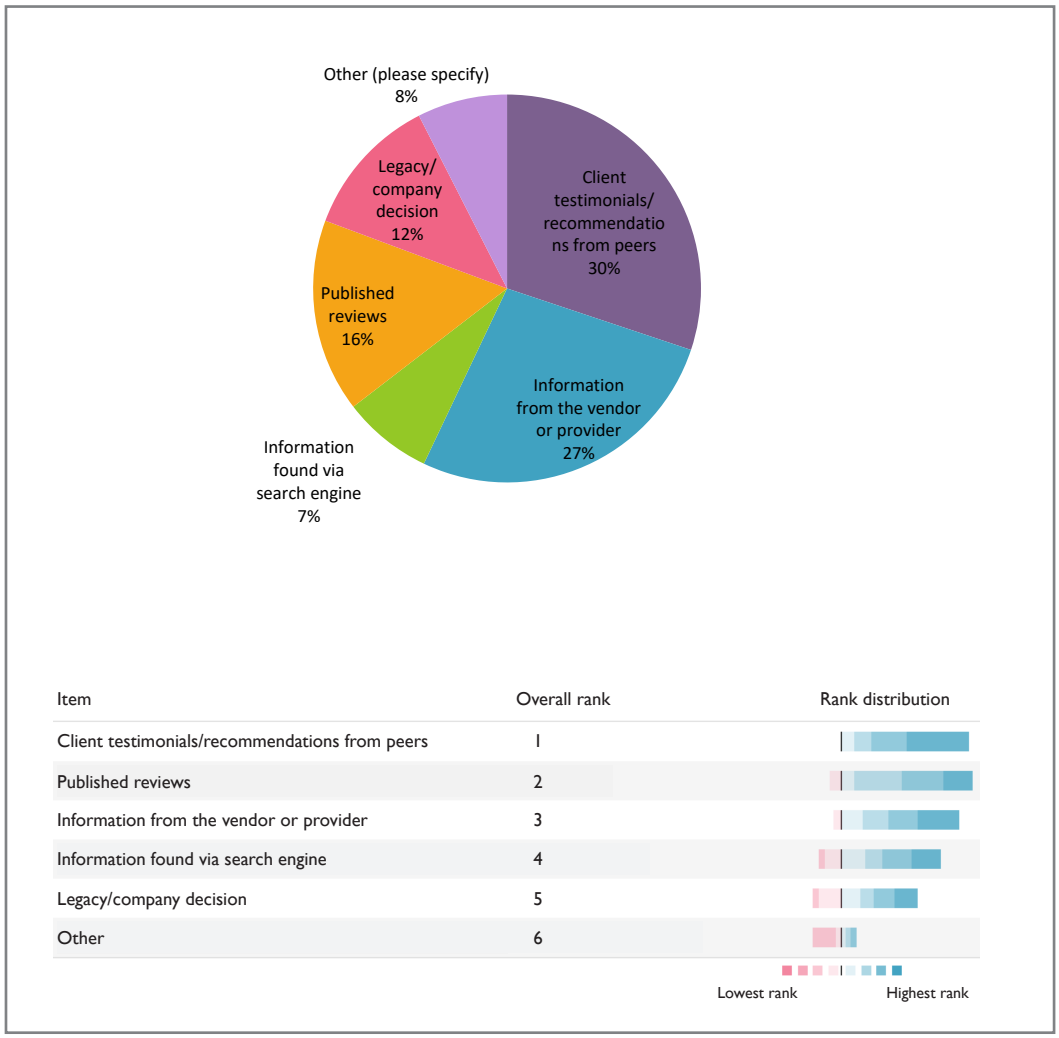
We also saw a strong divide in 'pro' and 'anti' MSSP participants in each 'demographic' question, all of which suggested that MSSPs were more likely to appeal to participants whose role was not exclusively cybersecurity focused, and who had fewer resources, smaller information security teams, and less experience in the field.

As well as asking participants about their priorities in a solutions provider, we also asked them what resources they relied on to evaluate whether specific vendors managed to fulfil those priorities. We initially asked them about the most important factor in choosing their current provider(s), and then asked them to rank the other factors which they considered.

In both questions, participants who wrote their own answers in the 'other' fields mostly mentioned POCs, with several others specifying analysis companies such as Gartner and Forrester.

We also had a few participants tell us that their primary consideration was long-term personal experience with the product or the vendor.

Direct conversation with our contacts also resulted in POCs being mentioned frequently as the primary source of information, though third-party analysis was specified most often as the key method of deciding which providers to approach for POCs.



The high percentage of participants who reported either client testimonials or information from providers as their primary source of information is very encouraging to us – though of course procurement decisions should take into account information from as many sources as possible, we are big believers in the importance of information-sharing between peers, and in transparent and direct communication between vendors and end-users.

Unfortunately, opportunities to gain insights in this way are often somewhat limited by one's own personal network of connections and availability, and can be especially challenging in regions with less regional presence from vendors, but we do our best to provide these opportunities at our events.

WHO STANDS OUT?

The findings seen in the previous chapter confirm what we have heard over and over from the market. Professionals in cybersecurity-related fields are 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	Cisco	16	F5 Networks
2	Fortinet	17	Check Point Software Technologies
3	Symantec	18	AlienVault
4	Help AG	19	Barracuda Networks
5	McAfee	20	ManageEngine
6	Palo Alto Networks	21	Qualys
7	IBM	22	LogRhythm
8	Trend Micro	23	PhishMe
9	Dell Technologies	24	Protiviti
10	Paramount Computer Systems	25	Forcepoint
11	GBM	26	Juniper Networks
12	Kaspersky Lab	27	Trustwave
13	Micro Focus	28	Darktrace
14	FireEye	29	Microsoft
15	Splunk	30	Quest Software

Votes for providers which are subsidiaries of or have been acquired by others on the list are included under the owner's name – for example, votes for Blue Coat Systems and Message Labs are included under Symantec, and votes for HP products are included under Micro Focus. The exception is Dell Technologies and VMware – though Dell is the parent company, VMware often operates separately and resellers typically sell its products under the VMware name.

This list keeps track of 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, though as we have seen these priorities were predominantly ease of integration, transparency, reputation and quality of customer support. 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 have had the most satisfactory experience overall.

The top thirty vendors named in this category are:

1	Cisco	16	PhishMe
2	Fortinet	17	SonicWALL Inc.
3	Palo Alto Networks	18	Trend Micro
4	Symantec	19	Alpha Generation Distribution
5	HelpAG	20	Barracuda Networks
6	IBM	21	Forcepoint
7	McAfee	22	Kaspersky Lab
8	Check Point Software Technologies	23	Splunk
9	F5 Networks	24	Tenable Network Security
10	Micro Focus	25	2-Sec
11	Juniper Networks	26	7Safe Information Security
12	Darktrace	27	Accertify
13	Dell Technologies	28	ACIS IT
14	GBM	29	Acumin Consulting
15	Paramount Computer Systems	30	BAE Systems

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. This is a major factor which must be taken into account when designing your security infrastructure: 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 that doesn't guarantee that they'll 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.

Risk area	Most effective
Network security	Cisco
Threat management / intelligence	Fortinet
SIEM / real-time threat analytics	Splunk
Endpoint security	Symantec
Email and messaging security	Symantec
Web security	Symantec
Incident response	ManageEngine
Industrial / SCADA / IoT security	Fortinet
Payment / transaction / eCommerce security	Mastercard Payment Gateway Services
Mobile device security	MobileIron
Identity and access management	Quest Software
Penetration testing	Help AG / Qualys [tie]
Cybersecurity training	PGI
MSSP	Dell Technologies / Secureworks

HELP AG
PROTECTING INFORMATION

Lock Your Digital Treasures – A Case for Data Encryption

Dr Aleksandar Valjarevic,
Head of Solutions Architecture, Help AG Middle East

Organizations in the Middle East work in a fast-paced and competitive environment. Data is the new oil, powering growth, efficiency and effectiveness. Translated into actionable intelligence using IT systems, data creates competitive advantage and regional organizations in both the Government and Enterprise sectors have been highly successful in using the power of data and information technology to achieve customer-centric innovation.

But, the volume of sensitive data generated by the modern enterprise is a double-edged sword. While it can be used to guide strategic decision-making and create personalized experiences for customers, it raises a troublesome question – what happens when data is misused? What happens when a breach takes place? In short, organizations suffer remediation costs, reputation damage, loss of business and more.

The average total cost of a data breach for organizations in the Middle East is $5.31 million, as found by research conducted by the Ponemon Institute[1]. This number reflects just how much of a financial impact a single data breach can have - a cost likely to cripple all but the largest organizations. Despite this persistent threat, only 30% of companies have a consistent encryption strategy implemented enterprise-wide[2].

How is it that this paradox exists and why has data encryption been largely overlooked in enterprise security strategies?

The inability to protect data also places obstructions in the way of successfully leveraging new technologies such as cloud, big data and artificial intelligence as along with their operational benefits, these also introduce new threat vectors and changing security paradigms.

Taking cloud as an example, if used securely it becomes a great enabling factor – organizations get access to more and richer features, powerful platforms and great software services, while being able to optimize their costs and move from CAPEX expenditure model to OPEX. However, cloud adoption changes the threat landscape. As platforms and applications are becoming more and more secure (vendors invest heavily in securing their cloud offerings), threats are moving to identity of end users, end-points (computers, smart devices) and data. With this changing security paradigm securing the data itself becomes so much more important.

'Locking the Doors' to Valuable Data

Organizations invest heavily in information security, creating layered security architectures and implementing various processes and technical security controls, yet they fail to consistently implement data encryption. If we draw comparisons between information security and physical security in a bank, not encrypting data would be analogous to not locking the bank vault. Yes, there are many physical security measures already in place – cameras, high walls, electric fences, many layers of doors, security

1 2018 Cost of a Data Breach Study
2 2017 Encryption Trends Research

guards, and motion sensors – yet one still needs to lock the vault!

The reason organizations overlook the essential digital 'locking' with encryption is the perceived complexity of introducing and managing this technology, and its assumed impact on business processes.

A Fine Balance

Achieving confidentiality, integrity and availability data is simply not enough anymore – IT teams need to ensure convenience for users, administrators and managers when implementing any kind of security control, and especially so when implementing data encryption.

At Help AG, our advice to enterprises is to implement data encryption solutions for all their sensitive data and in particular personal, financial, health, business operations, trade secrets and intellectual property related data. Also, any data leaving organizational boundaries – such as in the case of cloud services or the outsourcing of functions to third-party service providers – should be included in the encryption strategy. This will soon become a mandatory component of security architectures and businesses that fail to implement effective solutions will continue to be easy targets for attackers.

Criteria for Solution Selection

Once the data for encryption has been determined, it is essential to implement the right encryption solution. In addition to budgetary factors, there are many criteria which should be given due emphasis. While encryption is an open technology area, it is not without its standards and regulations so trusting proven, tested and certified solutions is a good start. This narrows the playing field, leaving you to then focus on ease of deployment and management – both of which are essential to ensuring adoption and actual utilization of the investment. To this end, a system which offers minimal impact on performance and business processes is also imperative as otherwise, it would be difficult to build a business case for the solution and push for enterprise-wide deployment.

From a technical standpoint, the solution must cover your organization's encryption requirements in multiple use cases and environments, from on-premise to the cloud, from big data to containers, and from application encryption and tokenization to database encryption. Besides meeting immediate needs, this is necessary from a future-proofing stand point. Also important to the IT team is ease of management and here a solution designed on open-standards simplifies integration with other critical security systems, thereby enhancing the overall security architecture, simplifying utilization and eliminating operational overheads.

Once all these parameters have been given their due consideration and appropriately fulfilled, the support of a skilled and trusted implementation partner offers the final piece of the puzzle, ensuring the solution is configured to the specific needs of your organization, thereby allowing it to be leveraged to its full potential.

By using encryption – both for data at rest and in transit – you can ensure your organization's sensitive information is kept safe while still providing all the benefits that the ready availability of quality data presents to the modern enterprise. ■

About the Author

Dr Valjarevic holds the position of Head of Solutions Architecture at Help AG, a leading Middle East provider of strategic consultancy, tailored information security solutions and services. He is a seasoned information security and management professional, passionate about effective information security solutions that assists organizations to gain competitive edge. Working experience from Europe, Africa and the Middle East. Experienced in system design and integration, project management, business development and business strategy. Recognized as a thought leader and published numerous scientific papers and professional opinion articles. He holds a PhD in computer science from the University of Pretoria and is Certified Information Systems Security Professional (CISSP) and Project Management Professional (PMP).

While in some categories there is a clear 'winner', in others the competition is considerably closer. This is particularly true of the 'IoT' category – while Fortinet received the most votes, it did so by a very narrow margin. Most vendors nominated received very few votes, and in fact the most frequent response was 'N/A'.

Despite what has been discussed earlier about the increasing importance of IoT and connected device security, particularly in cities embracing 'smart' initiatives such as Dubai and Abu Dhabi, follow-up interviews indicated that IoT security did not merit particular consideration beyond the normal parameters of endpoint security, and that employee-owned devices, even if used at work, were not necessarily part of the information security team's remit.

The same explanation may hold true for the relative lack of votes in the 'mobile device security' category, though in this category MobileIron did win by a substantial margin.

The 'identity and access management' category did receive more responses and a winner did stand out, but something which stood out to us was the high number of vendors who were nominated here but which only received one vote each.

We asked some of our contacts to comment on this, and were told that the available solutions – whether provided by third parties or managed internally – were not thought of as being highly differentiated in terms of effectiveness, and that the tools were often included in more general endpoint or network security products. As such, though the importance of identity and access management was recognised, no one solution stood out to our participants as particularly effective.

On the other hand, in some categories we did see clear favourites among our participants. Although 'network security' is the only category in which Cisco was voted most effective, it won 29% of the vote here – as 'network security' is perhaps the broadest category we asked about, Cisco's performance here likely reflects its reputation as a good all-rounder, which is also seen by its high rating overall.

Similarly, in the areas in which Symantec won, it consistently stood out ahead of its nearest competitor, with 29% of the vote for endpoint security, 23% for 'email and messaging security', and 21% for 'web security'.

However, it should be noted that in the email/messaging and web security categories, several of Symantec's votes were in fact for subsidiaries: a full two thirds of Symantec's votes in the 'web security' category refer specifically to Blue Coat.

In other categories we see two vendors standing out ahead of their other rivals: in the 'SIEM' category, for example, Splunk and IBM received 22% and 17% of the vote respectively, with the closest competitor achieving only 12%, and in the 'mobile device security' category MobileIron received 20% and AirWatch (a VMware product, though all voters left out 'VMware') received 15%.

We didn't differentiate between the creators of a solution and consultants or resellers when asking about vendors more generally, and this is reflected by the inclusion of resellers and consultants in our overall top thirty – and even in our top ten.

However, given the lack of on-the-ground support provided by vendors in the UAE, we also asked specifically about consultants and resellers:

Resellers – Product knowledge	Help AG
Resellers – Consulting expertise	Help AG
Resellers – Implementation efficiency	Help AG
Consultants – Product knowledge	Help AG
Consultants – Consulting expertise	Help AG
Consultants – Implementation efficiency	Help AG

These results speak for themselves, and their significance is enhanced by the fact that with many vendors having no UAE presence, resellers are a key resource for end-users.

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 vendor representatives directly (when possible) and running POCs can give a fairly good sense of the solution's applicability in these areas.

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. Therefore, we also analysed the distribution of votes according to factors such as industry, size of company, and the characteristics participants prioritised in solutions providers:

Industry	**Best fits priorities**	**Most mentioned**
Banking/Finance	Fortinet	Cisco
Government	Cisco	Cisco
Education	Cisco	Cisco
Travel/Hospitality	Fortinet	Fortinet
Retail	Palo Alto Networks	Palo Alto Networks
Oil/Gas	McAfee	McAfee
Construction	Symantec	Symantec
Healthcare/Pharmaceuticals	None	GBM
Trading/Manufacturing	IBM/Palo Alto Networks [tie]	Symantec
[All other]	Cisco	Fortinet

Size of company	**Best fits priorities**	**Most mentioned**
<100 employees	Help AG	Help AG
100-500 employees	Cisco	Help AG
500-100 employees	Palo Alto Networks	Cisco
1000-2000 employees	Cisco	Symantec
2000-5000 employees	Fortinet	Cisco
>5000 employees	Symantec	Cisco

Top three priorities include	Best fits priorities	Most mentioned
Variety of services offered	Symantec	Paramount Computer Systems
Reputation/client testimonials	Cisco	Help AG
Personal recommendations	Fortinet	Paramount Computer Systems
Quality of customer support	Cisco	Cisco
Transparency	Cisco	Cisco
Speed of response to new developments	Cisco	Cisco
Ease of patching	Check Point Software Technologies	Help AG
Affordability	Cisco	Fortinet
Existing client roster	IBM / Cisco [tie]	Symantec
Location of company [UAE]	Cisco / Fortinet [tie]	Cisco
Ease of implementation	Fortinet	Symantec
Integration with existing systems	Cisco	Cisco
Lack of need for additional staff resources once installed	Cisco	Cisco
Scaleability	Symantec	Symantec

Size of information security team	Best fits priorities	Most mentioned
0-2 individuals	Cisco	Cisco
3-9 individuals	Fortinet	Fortinet
10-20 individuals	Cisco	Symantec
21+ individuals	Cisco	Cisco

Role in company	Best fits priorities	Most mentioned
CISO / Information Security Manager	Symantec	Symantec
Audit	Cisco	Symantec
Information Security (other)	Cisco	Cisco
CIO / Chief Information Officer	Cisco	Cisco
Architecture / Infrastructure	Help AG	Help AG
IT Manager	Fortinet	Fortinet
IT (other)	Fortinet	Fortinet

Years in cybersecurity	Best fits priorities	Most mentioned
Less than a year	Check Point Software Technologies	Palo Alto Networks
1-3 years	Cisco	Fortinet
3-5 years	Cisco	Symantec
5-10 years	Cisco	Symantec
10+ years	Fortinet	Cisco

Perspective on vendor ecosystem	Best fits priorities	Most mentioned
Broadly negative	Fortinet / 7Safe Information Security [tie]	Fortinet
Neutral	Cisco	Help AG
Broadly positive	Fortinet	Cisco

Most important factor in choosing provider(s)	Best fits priorities	Most mentioned
Client testimonials / recommendations from peers	Symantec	Symantec
Information from the vendor / provider	Cisco	Symantec
Information found via search engine	Cisco	Fortinet
Published reviews	Fortinet	Cisco
Legacy / company decision	Cisco	Cisco
Other	Fortinet	Cisco

These cross-sections show that although factors such as company size or industry did affect participants' priorities, they did not necessarily affect which vendors were considered most effective.

We see the same core group from our overall 'top five' appearing over and over, but though we do see some differences in which vendors were mentioned, few others manage to overtake them for the 'most mentioned' spot.

The exception here is the high concentration of votes for GBM among participants in the healthcare/pharmaceuticals sector, which is sufficient to allow it to overtake 'big names' such as Cisco. Similarly, though McAfee was very popular with participants and came 5th overall in terms of mentions, it is only the oil and gas industry in which it takes first place.

Though there are very few examples where

"We really have to work together. Any vendor in the industry can put their solution on our platform. It doesn't matter if it's our licence or someone else's, our mission is to prevent cyber-attacks. Our main enemy is the cyber-criminals," Ercan Aydin, Director, Emerging Markets, Palo Alto Networks

the variation visibly affects which vendor has received the most votes in this way, we do see trends. For example, though Cofense (fomerly PhishMe) did not receive enough votes to be listed in the cross-sections shown on the previous pages, we noticed that it was particularly popular with participants involved in banking and finance – which makes sense, given the threat posed to financial institutions by advanced phishing scams.

This seems to suggest that though the 'big name' vendors such as Cisco, Symantec and Fortinet were voted for most frequently in the majority of categories, factors such as industry did produce variation in the overall results.

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 is 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, as we have seen with Symantec. 19% of Symantec's votes in fact named Blue Coat Systems or MessageLabs rather than Symantec, which may reflect the tendency to purchase through resellers rather than dealing with vendors directly, as it is unclear whether participants were aware that the companies they named were not independent vendors. It is also interesting to note that although Cisco received the most votes overall, Symantec was the vendor most ranked 'most effective' in the most categories – again, perhaps a result of its diversification through acquisition.

CONCLUSIONS

The rapid growth of the IT sector in the UAE has brought with it incredible opportunities to incorporate cutting-edge technology into businesses' IT infrastructure and the critical infrastructure of the nation.

The effect on the UAE's adaptability and ability to stand out as a global leader in terms of innovation and business has been phenomenal. However, while the speed of digital adoption has created an environment geared towards embracing new developments, this comes with some potential drawbacks. Innovations aren't just good for business – they're good for criminals, too.

With every new advance that's made, there will be someone trying to exploit it. In areas of security that have been around for a while, that's not such a big problem: we have well-established strategies and solutions in place that any professional should know inside-out. For newer technologies, security measures are struggling to keep up – information security professionals do not have as much training or experience with them, solutions for securing the area may not be as 'tried and true', and the flaws in the technologies themselves may not have been completely ironed out yet.

And as more and more devices – and people – become connected, there are more avenues for exploitation, meaning that not only IT professionals but the population more generally need to be aware of the risks posed by cyberthreats, and what can be done to safeguard against them.

However, as we have seen, one of the particular challenges facing the UAE is a lack of sufficient training. Due to an already limited workforce, a high staff turnover rate and rapid technological advancements, even IT and information security specialists may have difficulty keeping fully up-to-date with new developments.

And the UAE cannot afford to be complacent in this – cyberattacks are increasing worldwide, but Middle Eastern countries and the UAE in particular are extremely heavily targeted and are feeling the impact, suffering losses substantially greater than the global average.

What is really needed is a dramatic change in how board-level executives and senior management think of information security, matched by an equally dramatic change in how budget is allocated, particularly with regards to investment in staff.

Of course, this is a lot easier said than done, and the kind of shift in corporate culture, company-wide infrastructure, and broader understanding of technological risk that this would entail is likely to take years or even decades.

While the kind of paradigm shift we hope to see will have to be a long-term goal, there are measures that can – and seriously need to – be taken in the meantime. Perhaps the most striking observations to result from our research are the areas of security in which our participants did not answer, or even explicitly told us that they did not consider these areas relevant.

While direct contact has given us some explanations for the lack of responses in the identity and access management category, in other categories, particularly mobile device security and IoT security, the apparent lack of interest, knowledge or both is concerning.

Reports by cybersecurity experts indicate that the threats posed by these categories are

on the rise – Fortinet's threat predictions for 2018, for example, forecast a 'destructive' escalation of IoT-based attacks.[32] Kaspersky's analysis of the threats observed in 2017 and likely to increase in 2018 also predicts a rise in IoT-based threats, as well as in mobile malware.[33] If cybersecurity professionals have not been taking these threats seriously so far, they desperately need to start. ■

32 Fortinet, 'Fortinet FortiGuard Labs 2018 Threat Landscape Predictions'.
33 Kaspersky, 'Kaspersky Security Bulletin: Threat Predictions for 2018'.