Trend Study

Managing Security in the Digital Era

How are European businesses tackling a constantly changing landscape of persistent cyber threats and stringent data protection rules?

Paul Fisher
Research Director

March 2017

Gold sponsor

Computacenter

PAC
A CXP GROUP COMPANY

TABLE OF CONTENTS

TABLE OF FIGURES

Managing Security in the Digital Era

INTRODUCTION

Rising cybercrime, digital disruption and increased compliance demands are threatening the stability of businesses across Europe. Dealing with cybercrime alone is a challenge, but as businesses look for a competitive edge through digital, and with the General Data Protection Regulation (GDPR) just over the horizon, many are looking for outside help. Increasingly that help comes in the form of a Managed Security Services Provider (MSSP).

In other parts of enterprise organisations, long used to outsourcing (especially in the UK), it might come as a surprise that MSSPs are still seen as a relatively new concept and one that is still treated with suspicion by security chiefs. The issues are trust and control — handing over custody of the security of a business is not something to be taken lightly. It is that aspect of outsourcing that is often overlooked in the marketing and promises that a switch to an MSSP can bring. Trust and reliance remain key.

Still, there is now definitely a growth in MSSP adoption across Europe as the triple pressures of cybercrime, skills shortages and compliance take their effect on under-pressure IT departments, and boardrooms fret about the business impact of data breaches. So outside help is being sought.

That doesn't mean that any MSSP is going to get an easy ride. There are still barriers to overcome and buyers will remain to be convinced if they are to part cash for a first MSSP adoption, or an extension of an existing partial security outsourcing.

This major piece of research, conducted by PAC across industry gives us a detailed insight into the thinking of security professionals, and how they approach the serious process of outsourcing security functions to get the best possible solution.

The survey was conducted during February 2017 in the following countries: UK France, Germany, Nordics, Ireland and Netherlands. The field research questioned 200 CISOs, CIOS, CTOs and other C-suite professionals across manufacturing, retail, transport and services sectors.

Paul Fisher

Research Director, Cyber Security
PAC-CXP London

KEY FINDINGS

The **majority of European organisations** are now running some or all of their security operations with an **MSSP.**

More than 70% of organisations are **happy** with the MSSP they currently use.

MSSPs cannot be complacent. Those organisations that are looking for a replacement cite **lack of flexibility and expertise** as their **main issues.**

The cyber security skills shortage shows no sign of abating and is impacting heavily on choice of MSSP.

The **market** for MSSPs is becoming **fragmented** and a **pick-and-mix approach is emerging.** A significant 31% are planning to bring some security operations back in-house.

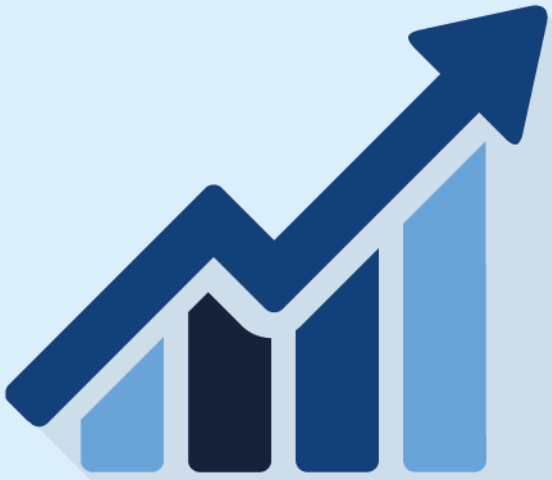
GDPR and compliance are low down on client lists of requirements. Just 20% of respondents see compliance as a major goal for any MSSP engagement.

Cost savings and efficiency still dominate management thinking. These were **major goals** of managed security services adoption for 69% of respondents.

Investment in MSSP usage will remain robust with 92% of respondents indicating an increasing or maintained level of investment.

The **key drivers of digital transformation** – cloud, mobility and IoT – are also the **biggest source of security concerns** for European organisations. Some 50% of respondents saw digital transformation projects as a threat in themselves.

Organisations believe that **in-house security teams are best able** to deal with advanced and nation-state attacks.



MSSP MATURITY AND STRATEGIES IN EUROPE

The first thing to note from our Trend Study is that Managed Security Services are now overwhelmingly established across European businesses, with 66% already using an MSSP, with a further 24% planning to invest. The remaining 10% are in the process of evaluating the prospect.

So it is maturing, but what does that 100% endorsement for Managed Security Services tell us? First, it is a bigger endorsement than PAC was expecting and demonstrates that across the board, on average, industry sectors are putting aside their reservations about using an outsourced security service. That said, the results within the sectors show that there is still some reluctance to fully outsource security.

If we dig a little deeper, we can see the option to outsource security is catching on, but there is still some way to go before end users completely trust an MSSP to fully manage its security. So 53% are at an early stage of planning with only 12% at an advanced stage.

For those already engaging an MSSP, some 71% are happy with the service they are already getting with no plans to replace, which means rival providers will have their work cut out preaching to the converted.

Given the level of commitment and trust needed to outsource security, this result could mean that the client is happy because nothing negative has happened, rather than 100% satisfaction with service and response. Engaging another provider is not to be undertaken lightly.

But clients *will* think about switching, especially if they believe that the provider does not demonstrate flexibility, or its expertise is found to be wanting. Expertise will be the great differentiator in the battle to win and keep clients.

Much lower down the list of reasons to switch are cost considerations, which suggests that end users want quality and security above savings. This is more than regular outsourcing. Security is seen as a worthwhile investment, perhaps over and above other IT investments. Given that the threat landscape is worsening and compliance burdens are increasing, this would make some sense. However, there is an anomaly in this result as we explain further in the report.

Clients *will* think of switching, especially if they believe that the provider does not demonstrate flexibility, or its expertise is found to be wanting. Expertise will be the great differentiator in the battle to win and keep clients.

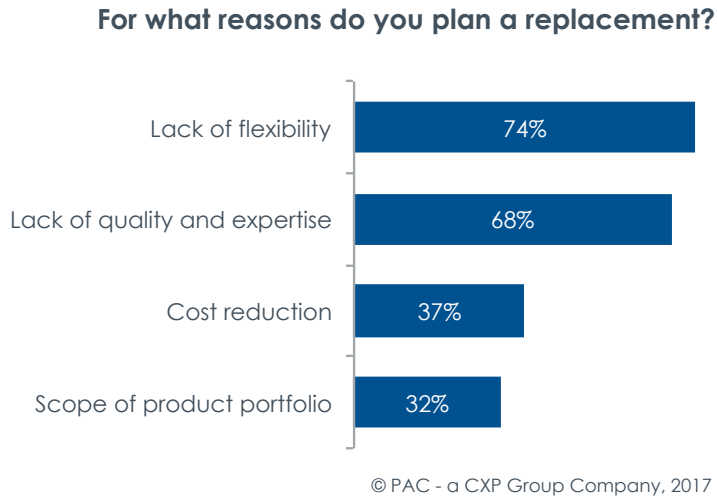


Fig. 1: MSSPs need to ensure they meet quality expectations or they could find themselves replaced.

For those thinking of changing MSSP supplier, a significant minority (31%) are thinking of taking operations back in-house because of the reasons mentioned above. This is an interesting result and, in PAC's view, not sensible or ultimately sustainable. PAC believes that only the largest and well-funded organisations can think about increasing on-premise security functions.

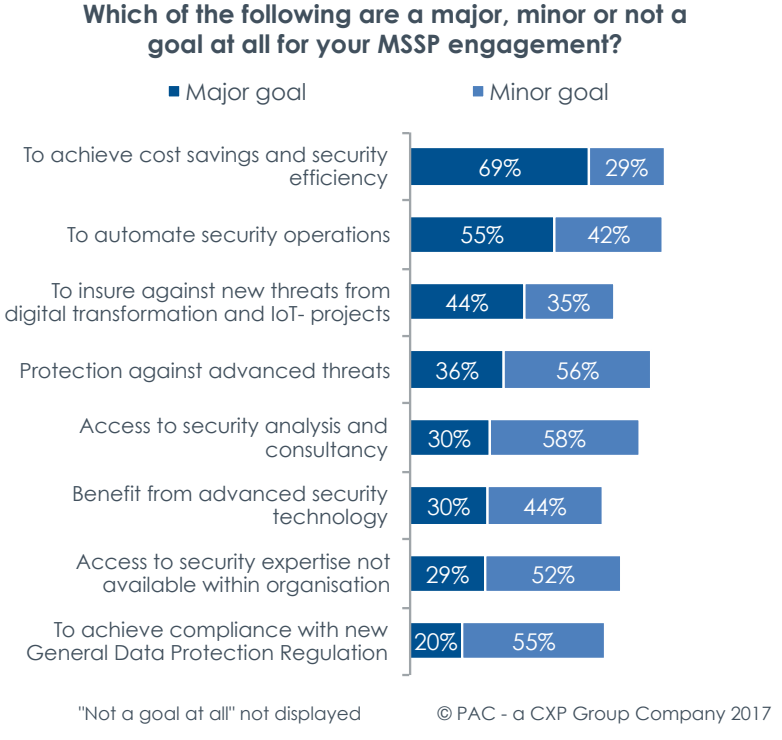


Fig. 2: When first appointing an MSSP, cost savings are overwhelmingly listed as a factor, probably influenced by C-Suite demands.

Why do European businesses seek the help of MSSPs?

So, here is our anomaly. While reducing costs is not listed as a driver for replacing an MSSP, cost savings and security efficiency are listed as the main driver for enlisting an MSSP in the first place. So, what is going on?

In PAC's view, the original impetus for engaging an MSSP could well originate from the C-suite looking to overhaul the security function on-premise and to indeed make an initial cost saving.

But once engaged, and the cost value of an MSSP has been achieved and recognised, there is less emphasis to reduce costs further. This is particularly so if management have seen that the MSSP has indeed managed security well, a new risk analysis records a better risk posture and actual cyber events are down.

However, the picture is complicated further by our respondents wanting to automate certain functions as well as insure against new threats. We can understand this. At the bottom end of the security technology curve are commoditised functions such as anti-malware software, firewalling and web filtering.

If an MSSP can offer reliable and cheap automaton of these as well as defend against more advanced options at the top of the technology curve, it could be onto a winner. Clearly, the market is looking for this to cope with complex threats and rising cybercrime.

Providers should also note the 30% of respondents who are looking for access to expert security analysis and consultancy, and the 29% looking for expertise not available in their own organisation (presumably not those also looking to bring security back in-house). As the cyber skills shortage continues to bite right across Europe, access to knowledge and strategic nous will be highly sought after by end users. But cyber skills are a rare resource, and getting rarer.

The challenge for the MSSP community is to compete for the best skills against each other, but also to some extent with their own customers. A lot will depend on the resources of the MSSP itself, some have more resources to recruit aggressively.

How do end users measure success for an MSSP?

Hiring an MSSP is just the start for many customers. They have determined their needs, looked at the options and are now looking forward to a more secure future and non-disrupted growth for the business.

But how do end users measure success? What are the likely KPIs for an MSSP? Does one actually include bottom line improvements?

An overwhelming 79% said that they do measure success. The number one reason is cost reduction, but, as mentioned earlier, this should be weighed against initial expectations and those more long term.

Look further down the list and there is a surprise. Some 68% said they are measuring improved staff awareness of security.

The idea that security is about people, processes and technology – in that order – obviously holds true. PAC finds this statistic highly significant as security awareness is often overlooked by the security industry, especially by an IT services sector so firmly focused on technology and process consultancy.

MSSPs should seriously think about adding staff awareness and training to their portfolios.

Given the close percentages of concerns such as raised security threats, data classification, and breach detection and response, MSSPs also need to contemplate these.

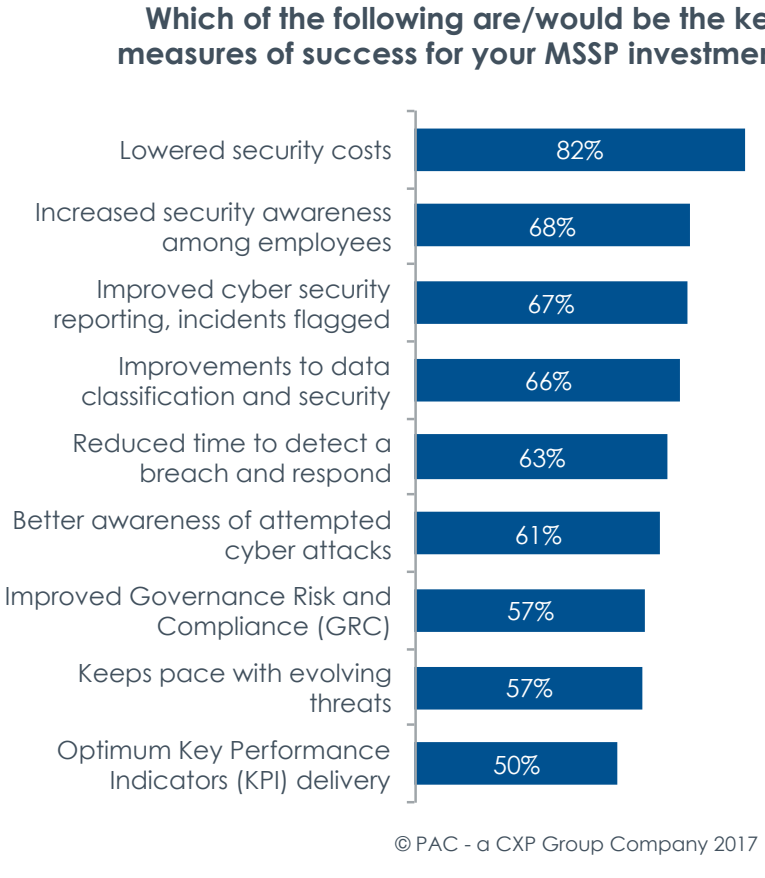


Fig. 3: Increased security awareness is a surprising measure of success.

GDPR is coming

Our survey was undertaken with 15 months to go before the EU General Data Protection Regulation becomes active in May 2018. Yet the results indicate very little awareness of how an MSSP could help an organisation cope with its impact.

Only 20% of respondents indicated that this was a good reason to employ an MSSP.

There are two ways to interpret this result. Either they do not see MSSPs as compliance specialists if they are thinking about GDPR, or they simply have not realised the impact that GDPR will have.

PAC believes that services in data classification will become more important for both providers and end users. Compliance with GDPR will only be legally registered if an organisation is able to identify exactly where data is, whether in its own data centres, in the cloud or with a third party. The data controller will be held responsible for data at all times.

GDPR will give national data protection authorities such as the Information Commissioner's Office (ICO) in the UK and the Commission Nationale de l'Information et des Libertés (CNIL) in France robust powers to punish those organisations that do not comply with GDPR. The big change is that organisations will be financially punished for violations of record keeping and privacy impact assessment obligations, and not just actual data breaches.

Organisations across Europe now face a huge task in putting their data in order before May 2018. PAC believes that many will need outside help with this and it is part of a trend where compliance and security merge.

An organisation that is compliant with GDPR is more secure simply by knowing where its data is located, and by extension where it may be vulnerable.

When asked in what ways an MSSP could assist in compliance with GDPR, 80% of respondents answered with "risk assessment" while 66% said "personal data classification and protection".

Both signify an awareness of compliance but PAC believes that they may have got their priorities wrong – data classification must be completed before an accurate risk assessment can take place.

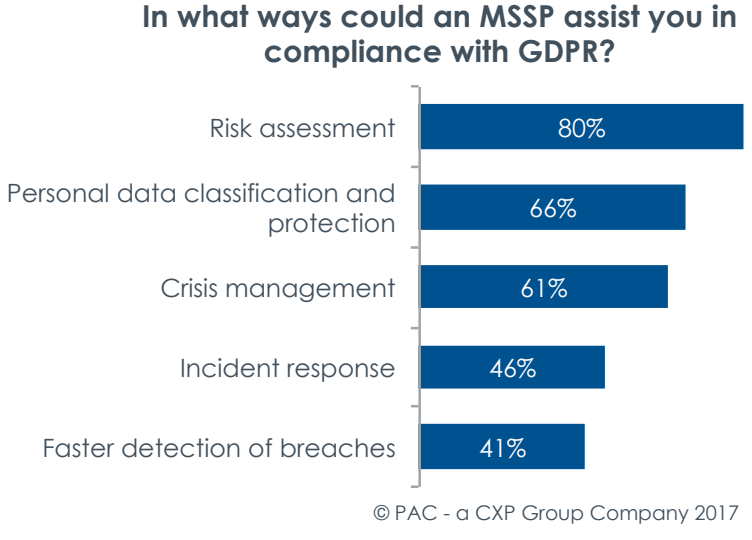


Fig. 4: GDPR will have an increasing influence over all security investment in the coming years.

Investment plans and areas of interest

One of the purposes of this report is to understand the penetration of the MSSP model into enterprises across Europe. The concept of a service model is nothing new in SITSI but the specific and high-level knowledge demands of cyber security and compliance make it something of a special case, much more so than simply outsourcing basic IT functions.

When asked about their level of spending on MSSPs in 2017, 55% replied between €1m and €5m while a significant 19% were looking to invest up to €10m. Whatever the level of spending today, 92% plan to maintain or increase investment in the next three years with 56% saying they will increase investment by 11-25% of current spend.

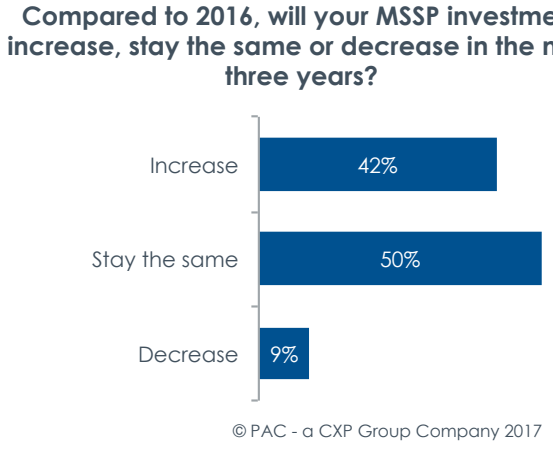


Fig. 5: There is no doubt that investment in MSSPs will grow further as this result demonstrates.

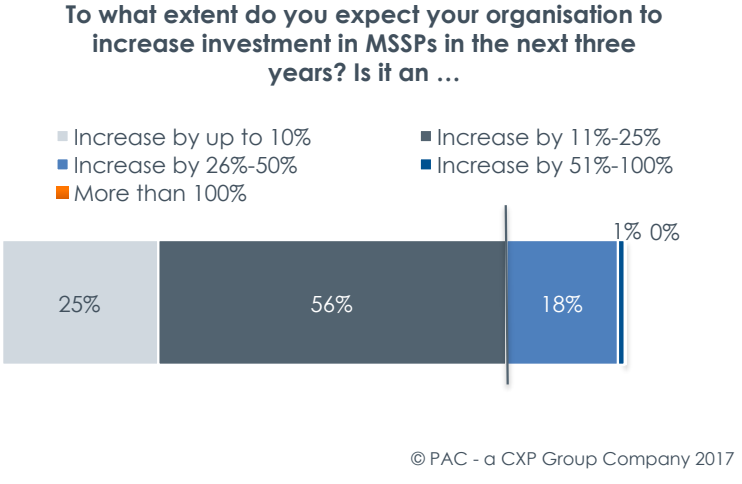


Fig. 6: Investment in MSSP will be steady, majority up to 25%.

When asked, in a multiple-answer question, in which areas of managed security services they would invest, 79% said they would invest in Threat Intelligence and Research, 56% said Security Asset

Management and Monitoring while just 38% were looking at Risk and Compliance Management.

Either our respondents already have compliance locked down (probably not) or they are more concerned about the state of their own assets' ability to detect threats. This comes back to our concerns about GDPR readiness.

Certainly, threat intelligence will help stop and prevent breaches, but it does not mean an organisation is necessarily more compliant. An improved risk posture can certainly be obtained by better Threat Intelligence on the ground but, in the new age of compliance, this can no longer be seen as a 100% risk assessment, unless you can also log your data.

CURRENT SECURITY AND BUSINESS CHALLENGES

To say that organisations face increased cyber threats is hardly news. We know that. What end users need and what MSSPs need to know better than their clients is how to manage these threats. So what are end users specifically looking for?

The results show that the trends they are most concerned about are also the drivers of change and innovation across European businesses. Our results confirm the feeling that the better things get in terms of digital transformation, the worse they get for security. So our respondents are most concerned about the following: mobile (74%), cloud (67%) and IoT (58%).

Other major IT trends such as digital transformation (50%) and shadow IT (34%) are also concerns (as they should be), but our results are a reflection of what end users are thinking about and dealing with right now.

While the media talk up cyber war or state sponsored attacks, very few respondents running important European businesses worry about it. Just 11%.

PAC's analysis is that these trends must not be obstructed (and probably cannot be) as within them lies the future prosperity and competitiveness of European organisations. Clients need to demand existing or future service providers to start thinking about how they can best manage and secure the digital future.

Attack, attack, attack!

Cyber security is fundamentally about stopping cyber attacks. In the age of nation-state sponsored attacks and the theory in some circles that types and classification of attack do not matter, the results here show that end users do still worry about specific forms of attacks – and how to stop them.

And, while the media talk up cyber war or state sponsored attacks, very few of our respondents, who run important businesses across Europe, worry about it (just 11%).

However, a significant 45% worry about what their competitors might get up to in the form of cyber espionage, which is of greater concern. Industrial espionage is as old as the hills, but now it is conducted through different methods – and one that MSSPs will be expected to prevent.

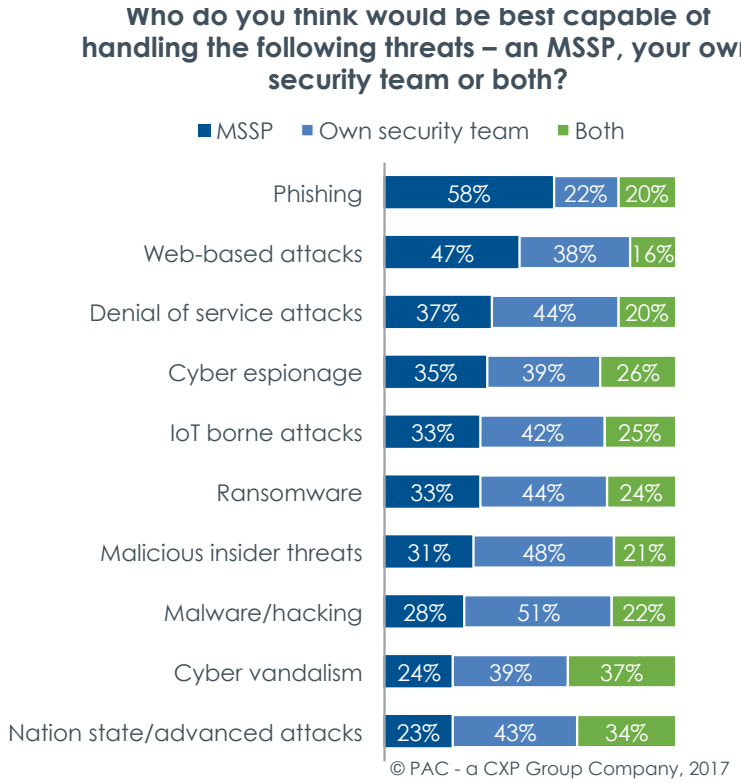


Fig. 7: Despite more sophisticated malware, phishing remains a highly effective form of delivery.

Of greater concern are conventional attacks such as malware, phishing and malicious insider threats – and the concern is, of course, that there are simply more of these types of attacks.

But any MSSP that can demonstrate real expertise in stopping malware will have an advantage. Spending time dealing with preventable malware attacks is a major waste of business time, and one that should really be prevented with near 100% efficacy by now. Any MSSP worth its salt must be able to operate towards this target.

So let's dig a little deeper and look at how those threats break down and who may be best at dealing with them.

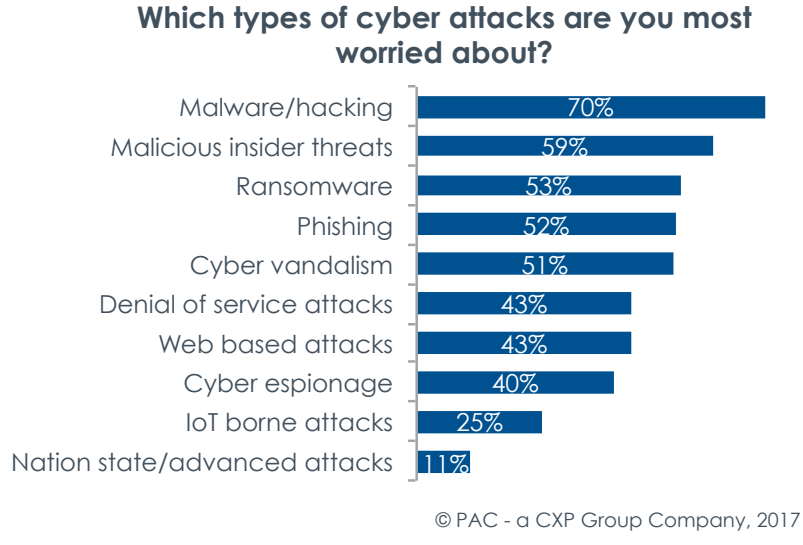


Fig. 8: Few in industry currently worry about the threat of nation state attacks.

This is where things get interesting and where MSSPs may have work to do to convince customers they are the people to call in.

Phishing attacks are considered the biggest challenge that MSSPs would be best equipped to deal with, which is interesting for two reasons.

One is that phishing is very hard to deal with and many breaches succeed through this entry method. Yet, in theory, better user education would stop phishing. Would MSSPs prevent phishing any better than in-house teams?

It's a difficult call. PAC believes that the results of this section are the answers to a different question in respondents' minds: *What are the most common attacks and which do you struggle to deal with most?* When put like this, the results make more sense, with phishing, web and denial of service being the most common and most damaging currently.

Advanced attacks, state-sponsored activity or cyber vandalism are deemed within the scope of the in-house team. Why? Simply because they do not happen very often.

The logic is: the less common an attack the easier it is thought to be dealt with by an in-house team – but this is not necessarily borne out by reality. Advanced attacks are probably most likely the hardest to

Advanced attacks, state-sponsored activity or cyber vandalism are deemed within the scope of the in-house team. Why? Simply because they do not happen very often.

WHAT DO END USERS LOOK FOR IN AN MSSP TODAY?

So far we have looked at the driving forces behind the choice of using an MSSP, such as the type and frequency of crime and of course compliance pressures. Of course, no MSSP or SITS business is going to say it is incapable of handling any of these pressures!

But what are end users expecting, what separates the men from the boys in the MSSP world? We certainly gave our respondents quite a menu of options to choose, from number of security experts right down to ease of communications.

What we were surprised at was that 69% of all respondents thought that the number of experts an MSSP can boast is a "must have", which says something about the effect the cyber skills shortage is having.

It also means there is a war between services providers to sign up the available talent, and prove they have the best.

The people doing the best out of this, of course, are those talented individuals who have the credentials and qualifications to get the best salaries and rewards. However, the shortage is affecting the compliance market too.

And end users are expecting more than just a knowledge of ISO 27001 – they expect soft skills such as excellent business communications skills, crisis management and delegation.

The second surprise was the desire that an MSSP have a global footprint – which will be a blow to smaller or more specialist security services players – but by looking at the vertical split we can see that the importance changes somewhat.

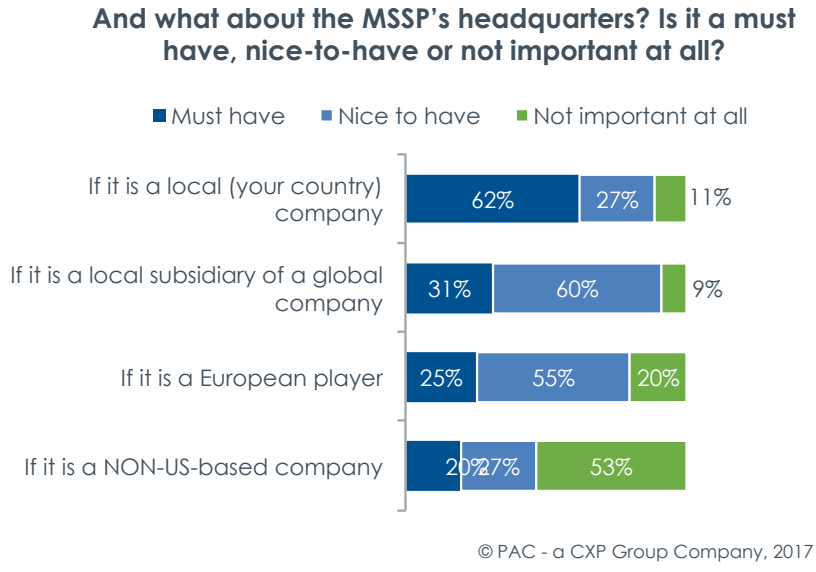


Fig. 9: Worries about consumer data has prompted a more local approach to managed security.

Local pressures are beginning to come into play in the form of compliance and pressure from consumers for their data to be better protected, especially in key EU markets such as France and Germany. Simply put, companies are expected to be fully responsible with data inter care, and that means that they are demanding geographic standards from their MSSP.

PAC believes this is the reason why 62% of all respondents see it as a must-have for the MSSP to be a local business, while another 31% want it to be at least a local subsidiary of a global footprint.

But, of course, this is slightly disconnected from their previous assertion that it should have a global footprint. Maybe there is hope for the smaller players after all.

They were more emphatic when it came to the location of the MSSP SOC – 63% want a local SOC while 23% wanted a non-US located SOC.

More bad news for smaller and specialist MSSPs. Security software providers are overwhelmingly preferred to pure plays, with general IT services players in the middle, while 6% trusted a global provider to meet their expectations and requirements.

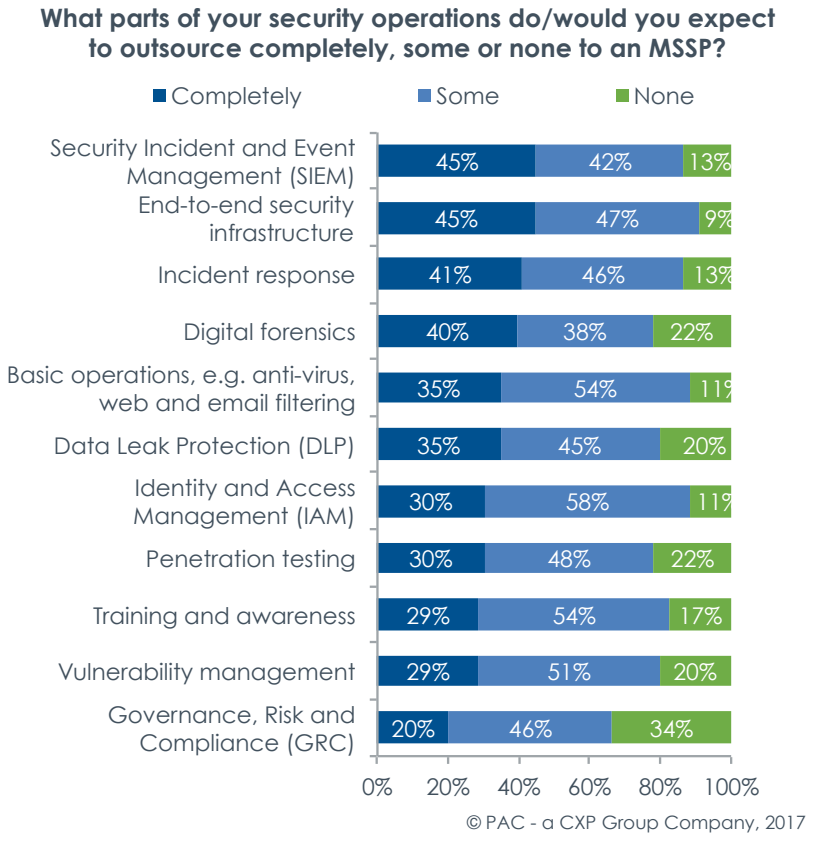


Fig. 10: Proactive approaches to security are gaining traction and incident management seen as essential.

We are not sure whether that is simply playing safe or that the smaller more specialist MSSPs have not got their message across yet. Either way there could be opportunities below the security software giants once GDPR gets underway, as this will need skills more commonly found within the Big Four accountancy firms, and local boutique security consultants who are software agnostic.

What areas would they outsource?

The picture here shows that end users are looking to the big players to offer expertise in areas which they do not necessarily have and are not always well equipped to deal with such as the SIEM, security response and forensics functions mentioned by survey respondents.

Fewer are looking to completely outsource commodity functions such as AV and firewalling, suggesting that the organisations are not able to find the skills and resources in-house to fight advanced threats.

The fact that more would want to deal with GRC in-house than completely outsource it is a worry and suggests again that European organisations are simply not aware of the implications and their responsibilities when it comes to GDPR.

However, when asked what concerns they have about using an MSSP, 61% said lack of visibility of data, but that is in all likelihood an expressed concern rather than an awareness of what lack of visibility might mean in terms of not meeting the basic requirements of GDPR.

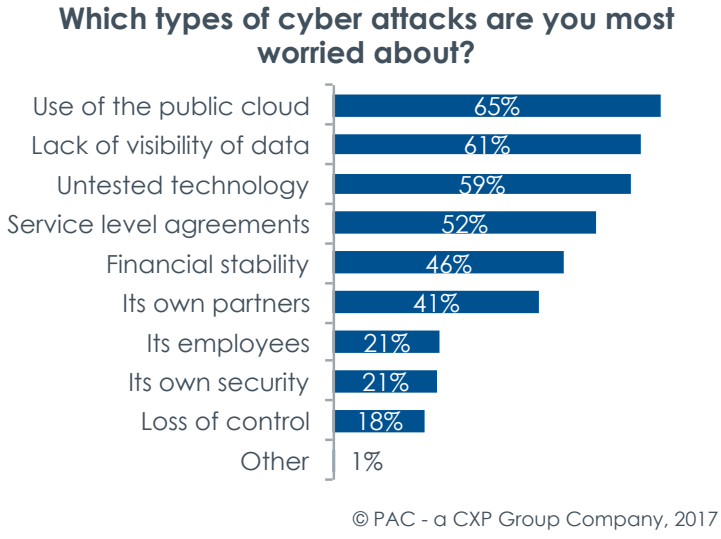


Fig. 11: Cloud is universally adopted but the security concerns have not gone away.

CONCLUSIONS

- Companies across Europe are becoming more comfortable with outsourcing security, even in sectors once thought hostile to using MSSPs, such as banking. But one size does not fit all. Clients and providers need to rigorously evaluate carefully which services and how they are applied.

- Compliance, and particularly the upcoming introduction of GDPR, figures low down on clients' security planning. In PAC's view, this is a significant oversight as a compliant organisation is also a more secure one. MSSPs can win by educating clients on compliance and by offering expert help, either on their own or through secondary partnerships.

- Client organisations have a mixed view of the benefits that an MSSP can provide, and different parts of the organisation have different expectations. The Board looks initially to save money and is happy when this happens, whereas the security teams look for help and technology that they cannot deliver in-house.

- An MSSP is not for life, or even for a whole organisation. Businesses are taking a pick-and-mix approach, and even taking some functions back in-house. MSSPs need to be flexible in terms of outlook and delivery. In an age of pay-as-you-go cloud and SaaS, they need to be agile enough to react to more frequent policy changes and new threats.

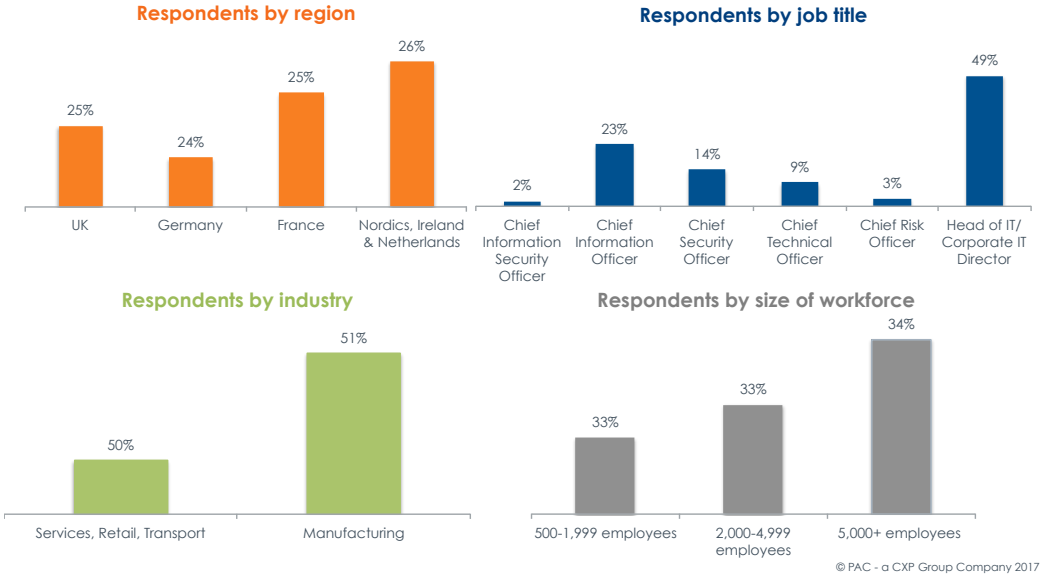
- Clients remain more trusting of larger IT services providers and traditional security software houses in their choice of MSSP. Smaller and bespoke players need not give up, however. As the demands of GDPR and advanced threats increase, clients may well look to more specialist providers, especially if they take a pick-and-mix approach.

- The on-going cyber security skills shortage is such that competition for security talent will put MSSPs at loggerheads with each other, as well as client companies. MSSPs will be under pressure to raise salary expectations while remaining competitive. In this situation, the client is likely to feel the benefit.

- Clients remain more concerned about conventional cyber threats such as phishing and malware and express a level of complacency with regards to nation-state or advanced attacks. MSSPs, however, should not take this as a reason not to offer advanced protection. Advanced techniques are trickling down the cyber eco system rapidly.

METHODOLOGY

The survey was conducted during February 2017 in the following countries: UK France, Germany, Nordics, Ireland and Netherlands. The field research questioned 200 senior IT and security job holders across manufacturing, retail, transport and services sectors.



ABOUT COMPUTACENTER

Computacenter is Europe's leading independent provider of IT infrastructure services. To help our customers maximise the value of IT to their businesses, we offer services and solutions at every stage of infrastructure investment.

Our ambition is to enable our customers, their businesses and their users by Making Digital Work. We do this by advising on IT strategy, supplying and implementing the most appropriate technology from a wide range of leading vendors and then managing it, as well as operating the appropriate IT services and support, on our customer's behalf. At every stage we help our customers to minimise the cost and maximise the business value of their IT expenditure.

Our corporate and government clients are served by offices across the UK, Germany, France, the Benelux countries, Spain and South Africa. We also serve our customers' global requirements through our extensive partner network.

For more information, please visit:

https://www.computacenter.com/uk/it-agenda/security

https://www.computacenter.com/uk/services-solutions/security

GOLD SPONSOR

Computacenter

Contact

Email:
communications.germany@computacenter.com

ABOUT PAC

Founded in 1976, Pierre Audoin Consultants (PAC) is part of CXP Group, the leading independent European research and consulting firm for the software, IT services and digital transformation industry.

CXP Group offers its customers comprehensive support services for the evaluation, selection and optimization of their software solutions and for the evaluation and selection of IT services providers, and accompanies them in optimizing their sourcing and investment strategies. As such, CXP Group supports ICT decision makers in their digital transformation journey.

Further, CXP Group assists software and IT services providers in optimizing their strategies and go-to-market approaches with quantitative and qualitative analyses as well as consulting services. Public organizations and institutions equally base the development of their IT policies on our reports.

Capitalizing on 40 years of experience, based in 8 countries (with 17 offices worldwide) and with 140 employees, CXP Group provides its expertise every year to more than 1,500 ICT decision makers and the operational divisions of large enterprises as well as mid-market companies and their providers. CXP Group consists of three branches: Le CXP, BARC (Business Application Research Center) and Pierre Audoin Consultants (PAC).

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

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

Follow us on Twitter: @CXPgroup

PAC - CXP Group
15 Bowling Green Lane
EC1R 0BD London
United Kingdom

Phone: +44 207 251 2810
Fax: +44 207 490 7335

info-uk@pac-online.com
www.pac-online.com

DISCLAIMER, USAGE RIGHTS, INDEPENDENCE AND DATA PROTECTION

The creation and distribution of this study was supported by Computacenter.

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

Disclaimer

The contents of this study were compiled with the greatest possible care. However, no liability for their accuracy can be assumed. Analyses and evaluations reflect the state of our knowledge in March 2017 and may change at any time. This applies in particular, but not exclusively, to statements made about the future. Names and designations that appear in this study may be registered trademarks.

Usage rights

Independence and data protection

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

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


PAC
A CXP GROUP COMPANY