VansonBourne

PRODUCTIVITY

Security is a team sport

Aligning stakeholders to strength IT security posture

David Gallichan
Account Manager

End user organisations, IT security vendors, and managed services/ security services providers (MSPs/MSSPs) must all be pulling in the same direction, or cyber criminals will win.

For the first two articles in our latest ProductivITy series looking inside the IT department, we've painted a stark picture when it comes to IT security. **External threats are rife, and appear to be on the rise**, while stretched internal resources, and **complications surrounding the IT security tools and vendors that organisations are using** – along with the apparent lack of a fully defined IT security strategy – all reflecting regular media headlines that cyber criminals are on the front foot, moving ever closer to achieving their corrupt objectives.

However, we're not here to preach about the rights and wrongs of what organisations are doing to protect themselves. Instead, in this third instalment, we will examine one possible option for organisations as, alongside their vendor partners, they look to stem the tide and elevate their IT security posture. This ray of light comes from the utilisation of managed services providers (MSPs)/ managed security services providers (MSSPs).

Embracing external support to alleviate internal issues

It’s true that sometimes too many cooks spoil the broth. In business that proverb can rear its head in various ways – whether too many people being involved in a process causes a decision-making bottleneck, or teams end up at cross purposes on a project, there are a number of ways where a smaller, more streamlined team can be of benefit.

And, in some respects, that may also be true when it comes to IT security. However, in an ever-evolving space, where knowledge and expertise definitely translate into power, surely the more brains there are working towards a common goal, the greater the chances of success when it comes to the good guys defending against cyber criminals.

The one thing to bear in mind here though, is that not all organisations have the expertise or the headcount in-house to throw towards IT and IT security needs.

How IT departments are structured across organisation sizes

Split by employee size	One department handling all things IT and IT security	One department, but with a team specifically focused on IT security	Two separate departments, one IT, one IT security	Individual/small "non-IT" team who manage needs through use of an MSP/MSSP	Other
Total	46%	33%	7%	10%	4%
1-49	49%	7%	0%	31%	13%
50-249	77%	10%	3%	10%	0%
250-999	61%	29%	6%	0%	3%
1,000-4,999	34%	53%	9%	3%	0%
5,000+	25%	55%	14%	3%	3%

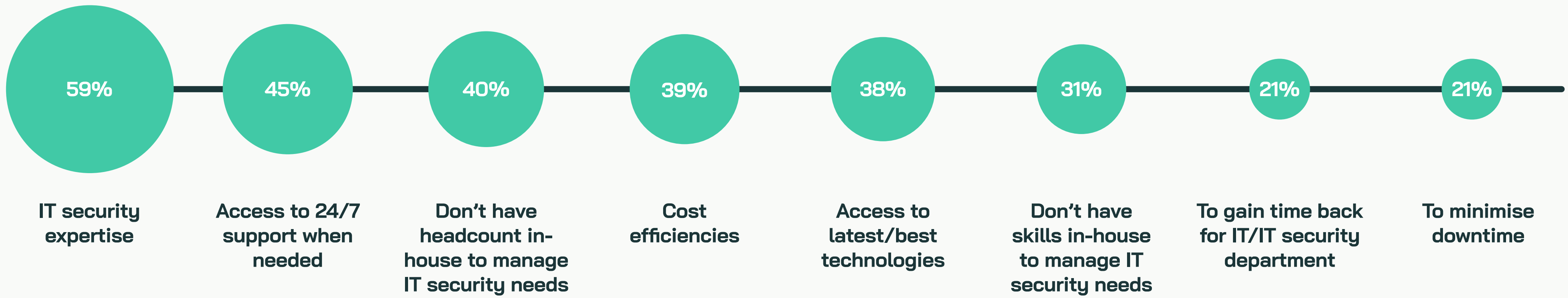
The way in which respondents' organisations' IT departments are structured begins to highlight these possible expertise and/or headcount shortfalls. As evidenced by the fact that larger companies (1,000+ employees) are notably more likely than their smaller counterparts to have one overarching IT department, but with this large team also including a group that focuses specifically on IT security – i.e., a team of dedicated experts exclusively working on keeping the business secure.

It is therefore probably fair to assume that the IT teams within the smaller surveyed organisations – particularly those with only 1-49 employees – are in a tricky position when it comes to both headcount and security expertise as they aim to maintain a secure environment for the rest of their colleagues. And this provides a good basis for explaining why these are the organisations most likely (31%) to be utilising an MSP/MSSP in tandem with an internal individual/small team to manage their IT security needs.

Sharing expertise and responsibility

But this doesn't tell the whole story – overall, almost half (46%) of surveyed organisations are leaning on an MSP/MSSP to some extent for their IT security needs, with this even applying to the largest surveyed organisations (5,000 or more employees) where 45% report that this is the case. Our two cents – this can only be a positive thing. As alluded to earlier, the more brains at the table working towards securing organisations the better, while it also highlights the value that these service providers can offer. This line of thinking is supported by the fact that 59% of respondents from organisations using an MSP/MSSP for their IT security requirements, report that the IT security expertise offered by these third parties is among the reasons for their use in the first place – making it by far the most commonly reported reason.

Key reasons for using an MSP/MSSP



Aside from the expertise that MSPs/MSSPs can offer, there is also the added bonus of easing the burden of responsibility on internal teams that are often already stretched and struggling from a skills perspective. This is clear from the fact that 40% and 31% respectively report that they don't have the headcount or skills in-house to manage their organisation's IT security needs.

These reasons tally up against the findings from the **previous edition in our Productivity series**, exploring people issues in IT today whereby recruiting the right skills – including cybersecurity – and having the right headcount were seen as among the key challenges for IT departments over the next 12 months. Not only that, but in this edition, around three in ten respondents cited an insufficient number of IT/IT security employees to do what is necessary (31%) and a lack of skills in the IT/IT security department (28%) as key challenges to their organisation's IT security currently.

It would, of course, be a stretch to say that without an MSP/MSSP organisations will inevitably fall victim to a security breach, but it stands to reason that the added support wouldn't go amiss. Further to that, it seems fairly evident that once a partnership is in place, end user organisations, IT security vendors, and MSPs/MSSPs must seamlessly work together if they hope to stave off the continuous barrage of threats that they're up against.

This is perhaps best demonstrated by the ways in which respondents' organisations keep up to date with the latest threat intelligence. Approaching half (48%) do so through their product vendors sending alerts on specific threats to their products, while only slightly fewer (43%) utilise specific threat intelligence tools from their vendors. And MSPs/MSSPs can also play their part by keeping end user organisations up to date with the latest intelligence, as is the case for 28% of those surveyed.

End user organisations clearly require assistance, so it's up to IT security vendors and service providers to help ease that burden and help to mitigate the risks at play.

How organisations gather threat intelligence

48%
Through product vendor alerts

43%
Vendor-provided threat intel tools

37%
Checking external vulnerability alerts

28%
Rely on MSP/MSSP to keep up to date

26%
Have an internal threat intel centre/ scouting team

Stronger together
- maximising IT security

All in all, the situation seems pretty clear – whether the partnership is just between the end user organisation and their IT security vendors, or whether there is also an MSP/MSSP in the mix as well, it is critical that all parties are singing from the same hymn sheet when it comes to maximising IT security efforts.

Security is, after all, a team sport, and until everyone involved recognises this and 100% buys into it, there will always be an avoidable opening in white hat security defences, with the damages of a breach having the potential to impact all of those who could have prevented it, to varying degrees.

Want to keep reading?

Explore the other articles from our latest ProductivITy series on cybersecurity:

PRODUCTIVITY

In the balance

How external threats and internal issues are complicating cybersecurity

David Gallichan
Account Manager

PRODUCTIVITY

Best tool or best vendor?

How organisations are building their IT security stack

David Gallichan
Account Manager

VansonBourne

COMMUNITY

The network for technology insight

These survey findings are based on qualitative and quantitative interviews with 216 members of the Vanson Bourne Community, our insight network of IT and business professionals at the forefront of their industries. We regularly engage with our members to tap into their expertise and perspectives on the latest technology-driven trends facing their organisations today.

Whether you're looking for deeper market understanding or data to drive your strategy, insights from our expert community can help inform your thinking and test your hypotheses.

Our Productivity database and insight series harnesses Community insights to take a forensic look into the IT department, investigating the issues faced by tech teams in ever-changing times. You've just read the latest in our ongoing series, exploring the cybersecurity issues in tech today.

Get in touch to learn more about these findings or to discover how the insights in our Productivity database can support your goals today:

Let's talk about research

VansonBourne

vansonbourne.com