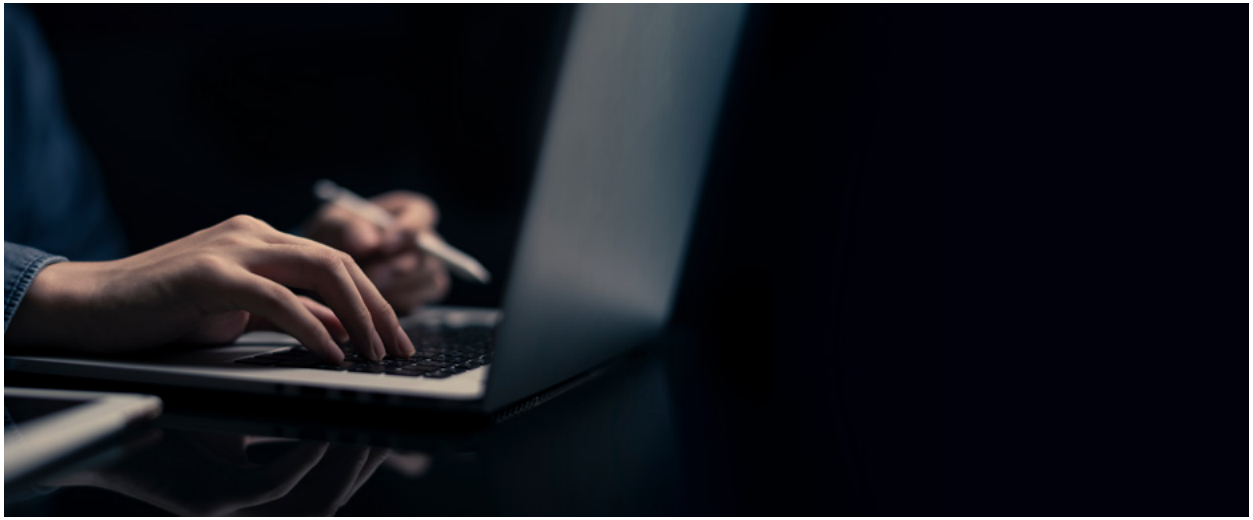
VansonBourne

PRODUCTIVITY

In the balance:

How external threats and internal issues are complicating cybersecurity

David Gallichan
Account Manager

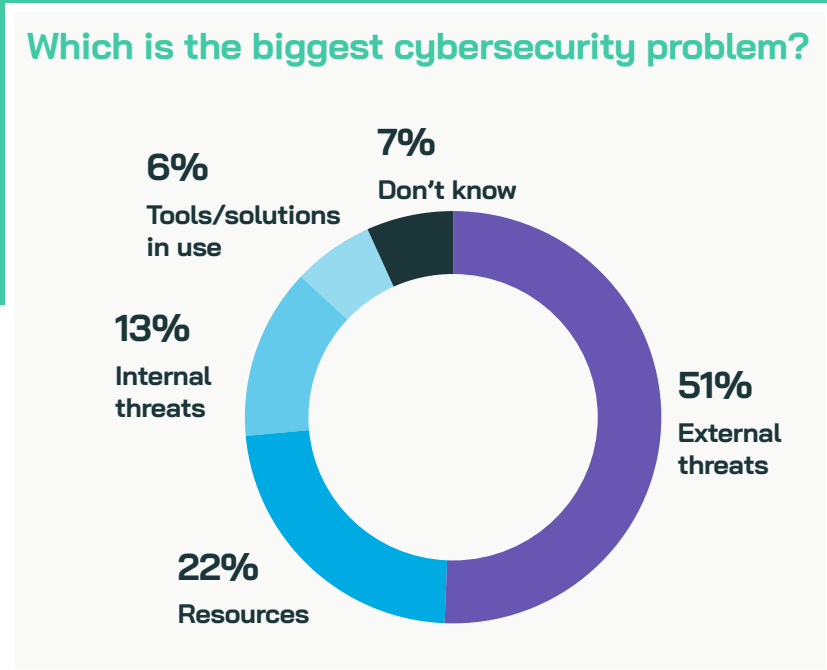


External threats to the IT security of organisations are pervasive, persistent, and proliferating, while internal issues further complicate the situation.

The world of IT security can be a thankless environment to work in – as evidenced by the **Chartered Institute of Information Security's 2020/21 State of the Profession report**, which found that 51% of cybersecurity professionals are kept up at night by the stress of the job and work challenges. Broadly speaking these work challenges can be grouped into two categories – internal difficulties, such as (sometimes) careless employees and an ever-increasing stack of tools to manage, and external difficulties like the ever-evolving threat landscape and the increasingly persistent threat actors who deploy these attacks.

Throughout the year, our six-part **Productivity** series takes an in-depth look inside the IT department at the trends and topics they face. In this second part, we focus in on cybersecurity across three articles - firstly we will primarily focus upon the external dangers. Those that come from cyber criminals with malicious intentions who often operate in the "Wild-West" of the internet – bandit country, if you will. And we will explore what IT and business decision makers believe are the biggest threats to their organisation now and in the future, and what they can do in response to threats from outside their perimeter.

External threats prevail, but internal issues can't be ignored



Media coverage in recent years – including this *TechTarget article* – will give you a good steer as to the scale of the problem that organisations are dealing with when it comes to cybersecurity. And, as such, it is perhaps of little surprise that 51% of surveyed decision makers believe that external threats are currently the biggest problem surrounding their organisation's IT security.

However, it is important to note that the remaining cited issues are internally focused, and therefore more than four in ten (41%) surveyed businesses have an internal problem as their biggest IT security challenge.

Arguably, in a strange way, external threats being the most significant issue should be where organisations are aiming to get to – implicitly this indicates that their internal struggles are slightly more under control, even if they aren't completely rectified.

For IT security vendors this situation potentially presents more of a strategic challenge in terms of how they're approaching prospect organisations and working with current customers. With external threats being the prevailing challenge, it would seem logical that shiny new security products are the answer. But when considering internal resource challenges and the struggles pertaining to the integration/management of security tools, it becomes apparent that end user organisations are likely to be looking for more of a partner when it comes to their ideal IT security vendor, rather than a supplier who is simply looking to sell them a new solution.

Caught between a rock and hard place:
Cyberattack volume and sophistication on the rise

Frequency of cyberattacks **62%**

ITDMs' greatest risks to their IT security over the next 1-2 years

55% **Evolution of cyber threats**

This pattern of external threats being seen as a critical IT security challenge is clearly here to stay, with concern levels in this area set to remain high for at least the next couple of years. Ultimately, this problem can be viewed through the lens of volume vs. sophistication, both of which are similarly concerning to respondents.

On the volume side of the coin, **62% of decision makers cite an increased frequency of cyberattacks as being among the top three greatest risks to their organisation's IT security over the next 1-2 years.** This is supported by the 54% who expect the number of cyberattacks, that their organisation is targeted by over the next 12 months, to increase – notably higher than the proportion (41%) who report that this has increased over the last year.

When it comes to sophistication, **more than half (55%) point towards the continued evolution of the cyber threat landscape as a top three IT security risk over the next 1-2 years.** Coupling these aspects together, it's easy to see how the challenge of external threats can breed feelings of "we can't keep up" or "we're always at least one step behind our adversaries".

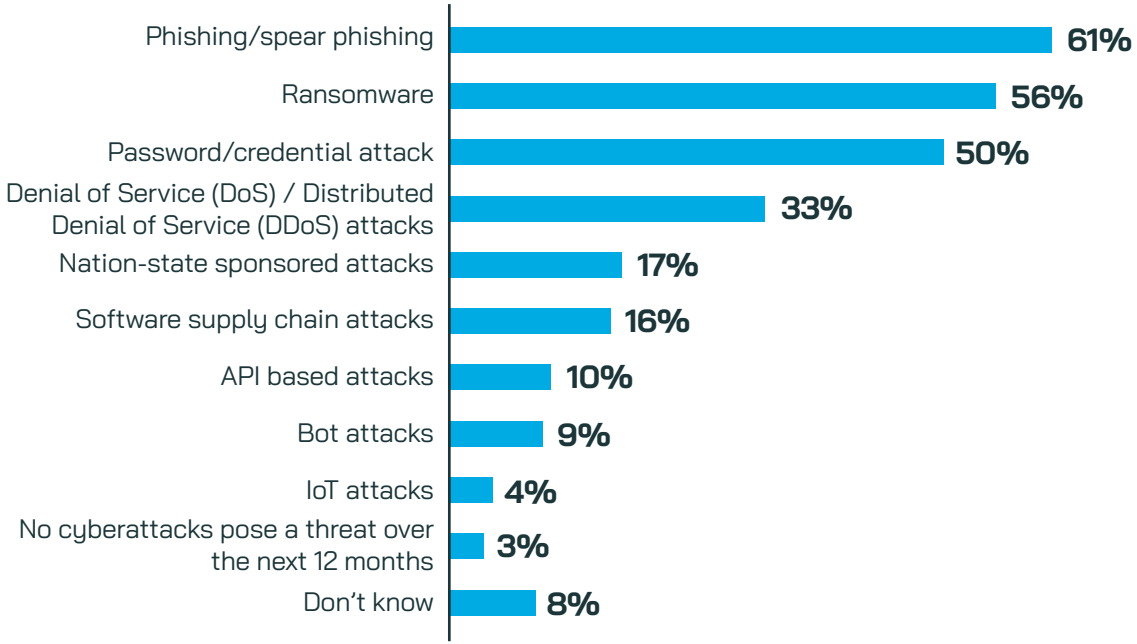
And, as the world has lurched from unprecedented event into further international turmoil, the challenges resulting from economic and political uncertainty are also seen as an IT security risk by almost 30%.

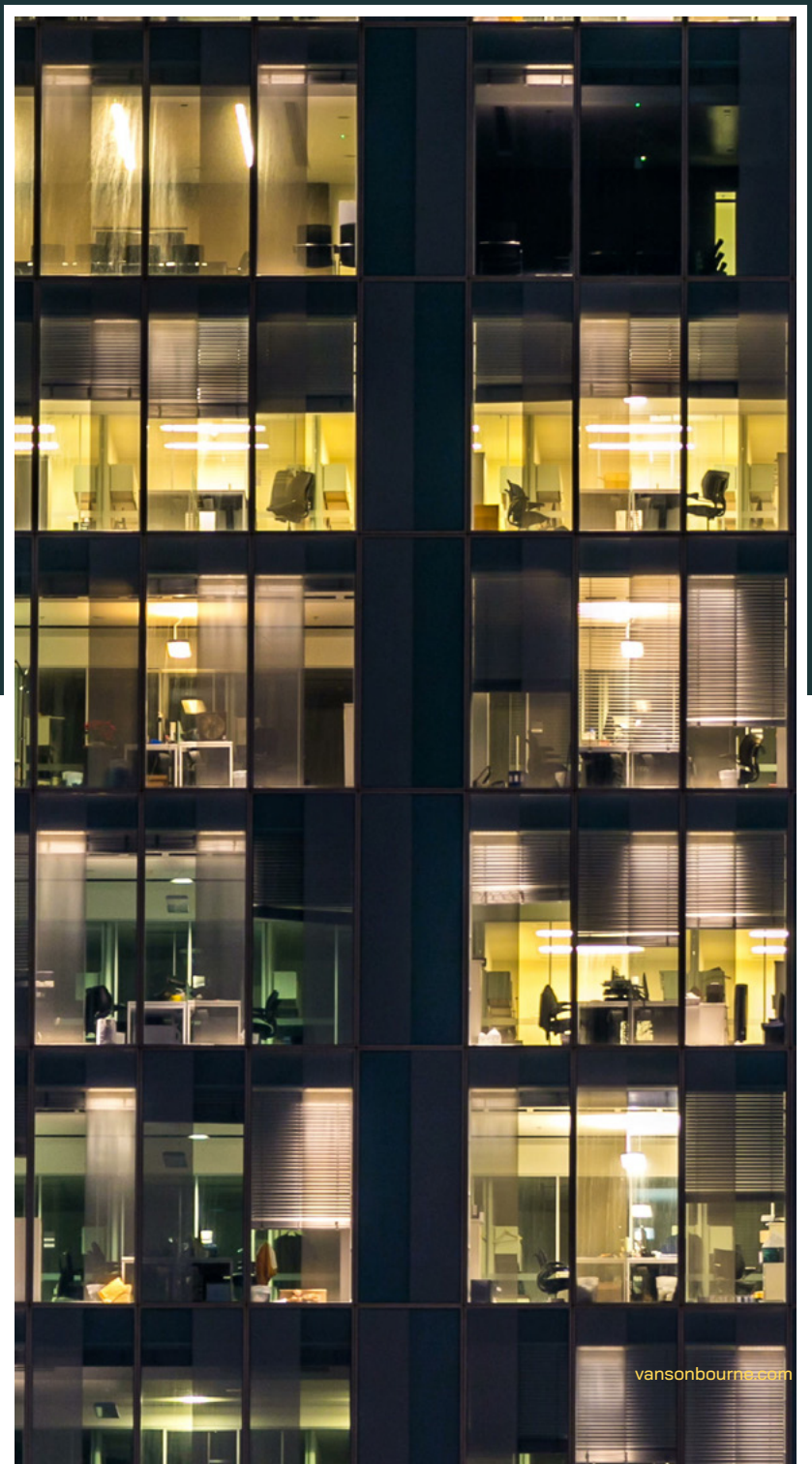
Typically, as humans, we're wired to fear the unknown. But the greater concern here is that, generally speaking, organisations seem to understand what's coming at them, and they already know that they're going to have a hard time dealing with it, making the role of IT security vendors increasingly important.

Mapping out the attack surface

In terms of the specifics, the attack vectors currently causing the biggest headaches at respondents' organisations, such as phishing/spear phishing (61%) and ransomware (56%), are probably the most well documented and the ones that security teams know the most about. However, this doesn't mean that they're easy to defend against, or that the same tools and skills required to effectively protect against these attacks are going to work in the face of the raft of other threats plaguing IT security teams.

Types of cyberattack that pose the biggest threat



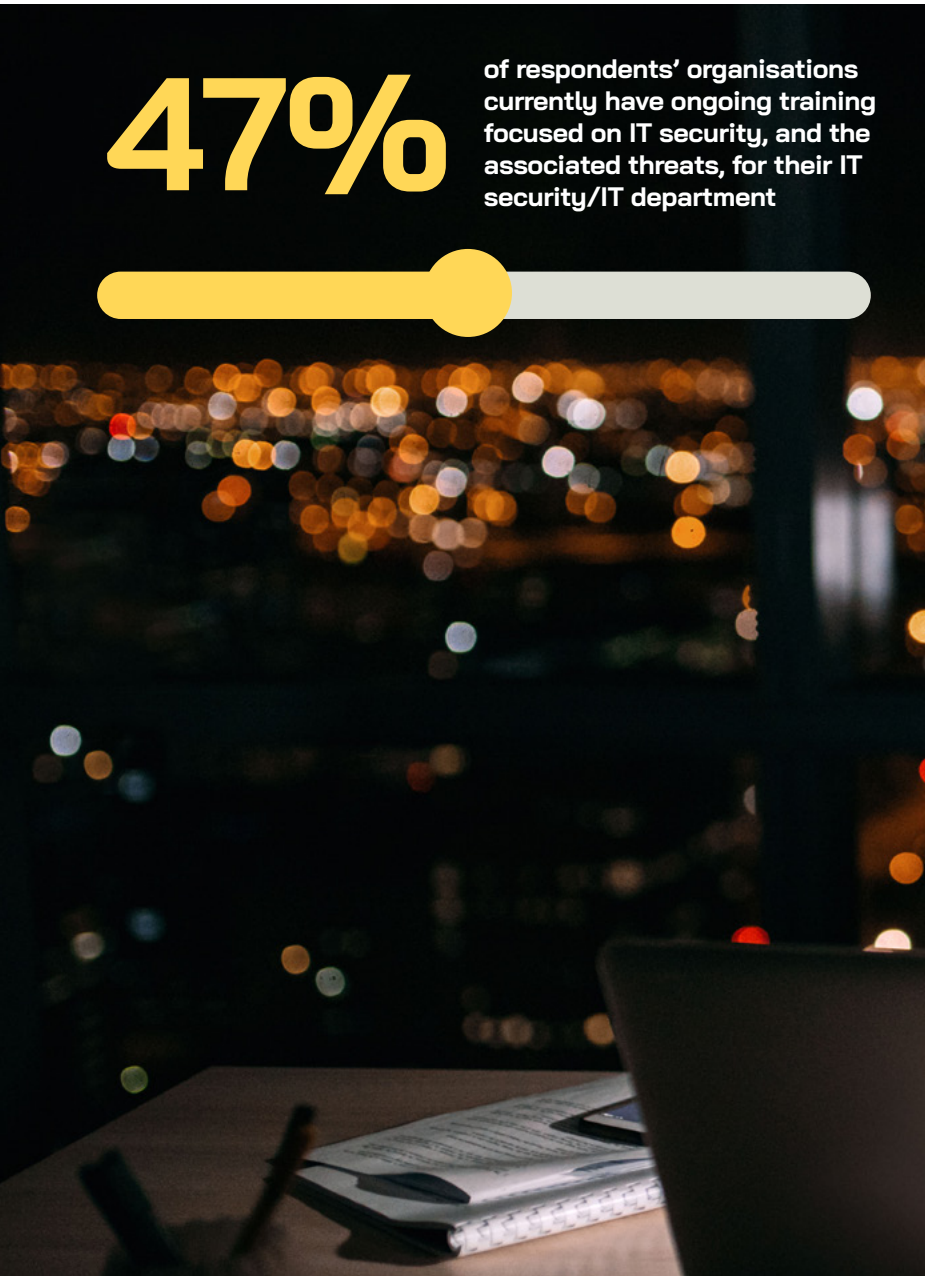


We can probably all think of multiple instances when we've received a phishing or spear phishing email, and we might also know what we should do when that happens. But, coming back to the idea of sophistication, the key thing to remember is that those perpetrating these attacks seem to be perfecting their craft – the emails are becoming increasingly polished, making it increasingly likely that an employee could fall foul of such an attack, thus the concern levels.

And, in recent years, ransomware appears to have become the attack vector of choice for individual cyber criminals, hacker gangs, and even nation-state actors. The financial repercussions for organisations coupled with the potentially destabilising impacts for critical infrastructure that ransomware can lead to, often mean that these are the attacks that make the most headlines – NotPetya, WannaCry, and Colonial Pipeline spring to mind immediately. But as those who have been stung will attest, it isn't "all bark, no bite", and its infamy is well earned, justifying fears around this form of attack.

So, the question is, how can IT security vendors assist organisations in combatting these external threats?

The starting point for the resistance



It's important for all involved in the fightback – IT departments, IT security vendors, and managed service providers (MSPs) alike – to remember that it's not too late to make changes that will improve the chances of rebuffing cyberattacks that have become something of an accepted inevitability.

A good place to start for organisations is to ensure that investment in IT security is plentiful and that spending plans are reviewed regularly. Reassuringly, of those who report that their organisation's annual IT security budget is expected to increase over the next 12 months, **59% say that it will grow more than their cloud technology budget, while 56% and 48% respectively report that IT security will over-index compared to budgets for software/applications, and data storage/ management.**

And, although spending isn't everything, it is a critical part of the puzzle, as is the implementation of appropriate training measures. Fewer than half (47%) of respondents' organisations currently have a formal, ongoing programme of training that focuses on IT security, and the associated threats, for their IT security/IT department.

Partner, not provider

There is a good chance that individuals within these teams do not have time, alongside their daily tasks, to keep themselves fully apprised of everything that is happening in their industry, so clearing time for them to learn can only be beneficial. After all, these individuals are the ones responsible for securing the rest of the organisation. How can they be expected to do their jobs effectively and, tangential to that, educate their non-IT security colleagues if they aren't enabled to keep up with the latest threat intelligence or defence measures?

For IT security vendors, this should be seen as an alternative way of partnering with new organisations and current clients. If they can provide further support than the provision of a new tool, such as threat awareness courses or security hygiene programmes for example, then they'll be delivering a more complete package that enables a more structured and effective security posture for their customers, while also taking a load off the IT department at the same time.

To defend against external threats, it's clear that organisations must first address practical measures that are controlled internally. Vendors and MSPs can help with this process – something that we'll explore further in subsequent instalments.

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