VECTRA®
SECURITY THAT THINKS

RESEARCH STUDY

Breaking Point:

Is mounting pressure creating a ticking time bomb for a health crisis in cybersecurity?

VECTRA
SECURITY THAT THINKS

Table of Contents

Executive summary

The struggle is real. The global cybersecurity skills shortfall now stands at 2.7 million workers globally, including nearly 200,000 in Europe and 33,000 in the UK alone. Exacerbating the issue, the global pandemic is rolling into its third year with no clear signs of ending. This is creating even more staffing demands – individuals are being signed off sick, while work from home mandates are disrupting traditional patterns, making many everyday tasks more difficult and time-consuming.

At the same time, the job of security is becoming more challenging. The bad guys are getting smarter; the attack surface is widening; and IT environments are becoming more distributed, complex, and opaque thanks to cloud and mass remote and hybrid working.

The cloud sits at the heart of much of this transformation. Whether it's transitioning from your own data centre to Infrastructure as a Service (IaaS) or using Virtual Desktop Infrastructure (VDI) to support remote working during Covid, the cloud has become an essential part of everyday business life. This change in IT strategy has triggered a major shift in how companies operate, altering the dynamics of risks that security teams now face.

This change in IT strategy has triggered a major shift in how companies operate, altering the dynamics of risks that security teams now face.

Cloud security skills are in short supply and teams lack the expertise to understand how to fully exploit the security features available in the cloud.

This new environment requires a different set of skills and tools to manage risk effectively and enable cyber resilience. Yet most of the new capabilities that are needed sit outside the traditional on-premises security toolset and knowledge space. This is driving a need to re-think the end-to-end security architecture to regain visibility. However, cloud security skills are in short supply and teams lack the expertise to understand how to fully exploit the security features available in the cloud.

Positively, the board and senior management are taking more notice, but investment can sometimes be slow to follow, putting extra strain on resources. Despite valiant efforts from security teams, these pressures are driving many in the industry to the brink. As this report reveals, these mounting challenges can have serious consequences – not just for enterprise cyber-risk exposure, but the wellbeing of security analysts themselves. From anxiety to depression, to panic attacks and sleepless nights, security professionals are at risk of buckling under the weight of responsibility. As the teams' health suffers, more people call in sick, creating an endless cycle of pressure – and the Covid crisis has only worsened the impact on mental and physical health.

As our use of technology continues to grow, and the threat landscape continues to worsen, we need to ensure that security teams' time is used in the most effective way possible. By thinking like our adversaries, making better use of automation, and using machine learning and AI to identify attack patterns in real-time, we can begin to alleviate the pressure and reduce cyber-risk. Automating routine and repetitive processes, searching for patterns that human eyes might miss and, crucially, prioritising threat alerts, can help to ensure that we apply human intelligence to the tasks where it is most needed. Security teams can dedicate themselves to more interesting work that inspires the mind, hunting for threats and helping to strengthen organisational resiliency – which can not only help to reduce analyst churn, but also ensure the right organisational context is applied to security threats to ensure the appropriate action is taken.

Key Stats:

- Almost a third (32%) have suffered a significant security incident in the past year – often negatively impacting team morale, causing arguments, and extending working hours
- Most (94%) security leaders have felt increased pressure to keep their company safe in the past year
- Half of security leaders say the pressure they are under is reaching breaking point – and they feel burnt out and ready to throw in the towel
- Over half (51%) have experienced negative emotions such as depression, anger, or anxiety due to feeling overwhelmed by work
- Two in five have had to seek help because of the physical impact of work-related stress – e.g., due to migraines, panic attacks or high blood pressure

By thinking like our adversaries, making better use of automation, and using machine learning and AI to identify attack patterns in real-time, we can begin to alleviate the pressure and reduce cyber-risk.

VECTRA
SECURITY THAT THINKS

Skills gap continues to exacerbate stress for SecOps teams

'The Great Resignation' has been trending in business circles for some time now. It refers to the sudden jump in staff turn-over that followed the initial stage of the pandemic – with employees becoming restless and looking for more from their working lives.

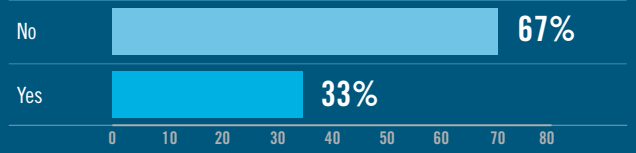
But the cybersecurity industry is no stranger to shortages. Even before the pandemic, the skills crisis was already taking a serious toll on Security Operations Centre (SOC) teams, with widespread vacancies going unfilled. Over two-thirds (67%) of security leaders told us they don't have enough talent on their team, 17% of whom say it feels like each person is doing the workload of three.

> With cybersecurity talent becoming harder to find, retainment is increasingly essential for the health of our global economy.

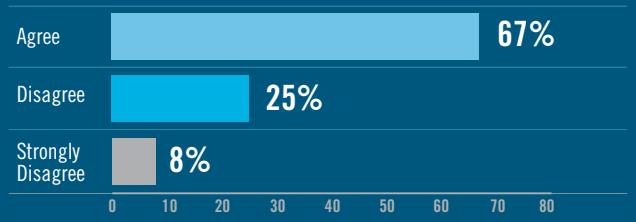
With cybersecurity talent becoming harder to find, retainment is increasingly essential for the health of our global economy. Without cybersecurity, planes cannot fly, money will not move, hospitals cannot heal. Yet constant under-staffing is heaping pressure onto existing teams, forcing cyber pros to work longer hours – often without extra pay. In fact, 67% are working more hours than ever but say they are still not able to cover their workload. Furthermore, **62% said they are in constant fire-fighting mode, making them very anxious**.

Worryingly, this is leading people to burn out. Our research shows that half (50%) of security leaders feel the pressure they are under is reaching breaking point, and they feel ready to throw in the towel.

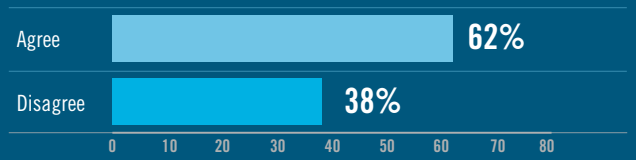
Do you have enough security talent on your team?



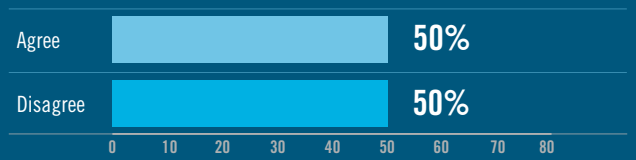
I am working more hours than ever and still don't seem to be able to cover my workload



I am in constant fire-fighting mode which makes me very anxious



The pressure I am under is rising to the breaking point – I feel burnt out and ready to throw in the towel



VIEW FROM VECTRA

Steve Cottrell, EMEA CTO on closing the skills gap

Addressing the skills challenge is tough, but there are many reasons to be hopeful, and there are practical steps that can be taken to bridge the gap. It is vital that we invest in education at the grassroots, so that school leavers are already thinking about a possible career in cyber. Opening the field to those without university degrees will also ensure we do not exclude potential cyber superstars who may be better suited to learning on the job than in the classroom. Something as simple as having school leavers trained on the common cloud platforms at a basic level would make students immediately employable and useful, and not take a huge amount of time.

> Opening the field to those without university degrees will also ensure we do not exclude potential cyber superstars who may be better suited to learning on the job than in the classroom.

We also need to consider 'supply and demand' and reward accordingly. Too often, cyber security salaries are pegged to IT salaries, which fails to recognise the extra layer of specialist skills required to perform the roles. Rises in wages will certainly incentivise more people to enter the industry.

Not only that, but organisations also need to rethink the SOC to make it more of a career destination. By providing career progression options *within* the SOC, we will gain a good mix of experience and new blood. Having this support and experience within the team will not only help to ensure that threats are properly mitigated; it will also encourage greater retention and training to upskill the team at large.

Finally, we can help to reduce the burden on security teams by reducing the amount of dull, repetitive tasks that can drag security teams down by automating the mundane and investing in tools that prioritise user-experience. This allows security teams to focus on the things that matter – as opposed to trying to spot the needle in a stack of needles.

TOP TIPS

- **Widen the net** – not everyone has to have a degree to be a cyber superstar
- **Make the SOC a career destination**, not just a jump off point
- **Automate data-rich tasks** to help security teams focus on high-priority incidents

VECTRA
SECURITY THAT THINKS

Changes to IT environment creating new threats

It is not only the skills shortage that is piling pressure onto cybersecurity teams; the rapid acceleration of IT adoption has also expanded the attack surface. Investment in cloud infrastructure and services; the enablement of remote access to the business's most critical databases and systems; new systems required to identify and verify users in remote locations – this has all led to an increase in complexity that is clouding visibility.

From oil pipelines and food supply chains to software companies, it seemed like no sector or organisation was safe in 2021. As new threats emerge, security teams are faced with the challenge of understanding what they mean for their business and reevaluating security strategies to meet their new challenges. It is perhaps unsurprising that most (84%) respondents said they have had concerns about cyber-attacks within their supply chain that could hurt their organisation and a further 91% have had concerns over ransomware. For some, these concerns are having a negative impact on wellbeing. 15% of respondents said they worried so much about supply chain attacks that it was keeping them up at night, while 13% said the same of ransomware.

It is not only the skills shortage that is piling pressure onto cybersecurity teams; the rapid acceleration of IT adoption has also expanded the attack surface.

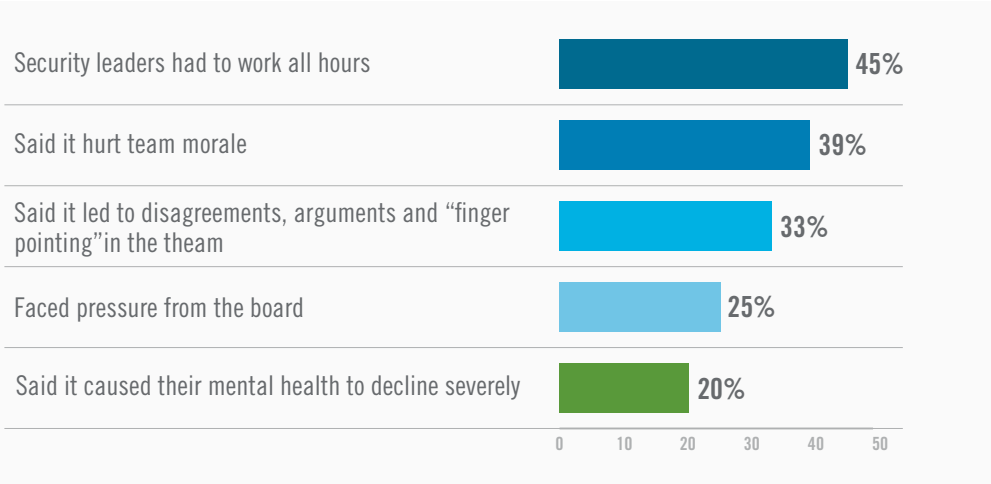
84% said they have had concerns about cyber-attacks within their supply chain that could hurt their organisation

15% said they worried so much about supply chain attacks that it was keeping them up at night

VECTRA
SECURITY THAT THINKS

Another key contributor to these feelings of anxiety is the growing lack of visibility. 92% of respondents said they've been worried about their ability to spot legitimate threats amidst a growing volume of security alerts. A further 90% said they'd had concerns that cloud adoption was adding to IT complexity and mounting cyber-risk – a legitimate concern, given the ease with which compromised logins can be bought on the dark web, or else stolen by phishing attacks. Social engineering can even persuade enterprise users to download apps to bypass multi-factor authentication (MFA).

Perhaps they are right to worry, as almost a third (32%) of security leaders we spoke to confirmed that they'd suffered a significant security incident over the past year. This is clearly taking its toll on SecOps. Of those that suffered an incident:



Social engineering can even persuade enterprise users to download apps to bypass multi-factor authentication (MFA).

92%

said they've been worried about their ability to spot legitimate threats amidst a growing volume of security alerts

90%

said they'd had concerns that cloud adoption was adding to IT complexity and mounting cyber-risk

32%

confirmed that they'd suffered a significant security incident over the past year

VIEW FROM VECTRA

Steve Cottrell, EMEA CTO on boosting visibility to increase confidence

When we think of enterprise risk, at a top level, it all comes down to the CIA triad – confidentiality, integrity, and availability – the three principles that guide cybersecurity strategy. Yet while risks may remain constant, the environment in which these risks are assessed and the threats that businesses face are constantly evolving. The technologies and techniques that were effective last year may not be the most effective in the new environment.

Often anxiety comes when we are facing a problem we don't have clarity on. That's life in security, where environments are complex and attackers frequently change their approach. Today, every aspect of the enterprise – physical and virtual – is under attack; down to the very code we build with, as seen with Log4j. This is where having a threat-led approach to security can be useful. By having a view of the top threats that are likely to impact your business, you can prioritise investment that will help build resiliency to those specific risks, allowing you to prevent, detect, respond and recover in a more effective way.

Often anxiety comes when we are facing a problem we don't have clarity on.

Yet while it's obviously important to limit the chance that an attack will be successful, the reality is that not all attacks can be prevented. If we want to stop ransomware attacks from being so profitable, we need to ensure that they are recoverable without having to pay the ransom. Having a strong

By having a view of the top threats that are likely to impact your business, you can prioritise investment that will help build resiliency to those specific risks, allowing you to prevent, detect respond and recover in a more effective way.

business continuity and recovery plan is absolutely critical. For example, regularly practicing recovery of key systems and routinely building in infrastructure and systems resilience to enable recovery from a ransomware disaster – or any other natural disaster.

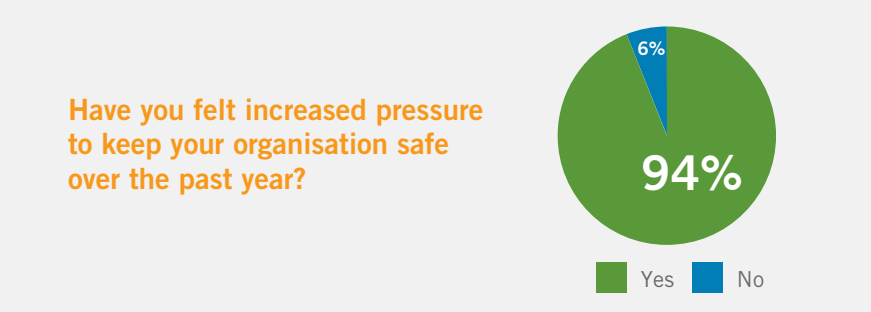
TOP TIPS

- **Constantly re-evaluate security strategy** to align risk to changes in the environment
- **Boost visibility through detection** to prevent attacks turning into breaches
- **Build strong business continuity plans** to enable fast recovery from breaches

As pressure mounts, the impact on security teams' health is worsening

IT and cybersecurity now sit across the entire business, integral to everything – from HR to finance – meaning if there is a problem, it has huge and very public ramifications. This is putting growing pressure on SOC teams to ensure network breaches don't escalate into major incidents.

The average cost of a data breach rose to over $4.2m in 2021, the highest in the 17 years since records began. It's no surprise, therefore, that almost all (94%) responding security leaders have felt increased pressure to keep their company safe in the past year. And that pressure is often coming from the top; 88% said that they worried about pressure from the board to keep the organisation safe.



Yet while the pressure is ever-present, many teams are being stifled by a lack of investment. Cybersecurity teams still find it hard to communicate their value or measure effectiveness in a way that engages the business, making it harder to secure vital funds. This puts teams at a further disadvantage – unable to pay the wages that will help them secure top talent and unable to invest in the tools that will provide them with the confidence and visibility needed to fight modern threats. This forces security teams to constantly do more with less.

88%

said that they worried about pressure from the board to keep the organisation safe.

IT and cybersecurity now sit across the entire business, integral to everything – from HR to finance – meaning if there is a problem, it has huge and very public ramifications.

Unfortunately, this pressure and under-funding is taking its toll on the health and wellbeing of security teams. The research revealed some sobering insights into the heath of cybersecurity professionals that could see us driving even more people away from the industry, at a time when we need to be pulling people in:

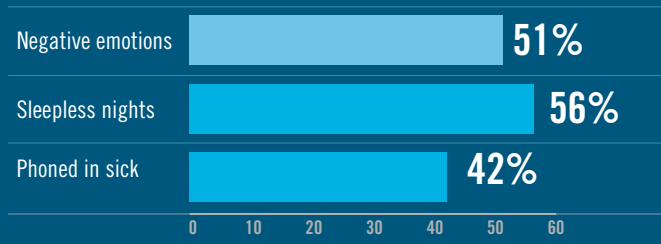
- **Over half (51%) of respondents have had negative emotions** – such as depression, anger, or anxiety – because of feeling so overwhelmed by work
- **56% have had sleepless nights** worrying about work
- **42% have dreaded going into work** and have called in sick because they couldn't face working

This stress is manifesting itself in physical health issues for workers too, with over two fifths (41%) of respondents saying they have had to seek help for work-related stress due to issues such as migraines, panic attacks or high blood pressure. These are serious conditions that could lead to people being signed off with long-term illness, along with major upset not just to the individual but also to the wider team.

These findings show us that the industry could be slipping into a health crisis. This should worry boardrooms and security leaders everywhere. Stress isn't just bad for the individual; it ultimately increases the risk of financial and reputational damage for their employer. Research shows stress can lead to poor decision-making – parts of the brain associated with emotion light up while those linked to memory retention weaken. In a security context, poor decision-making could increase the likelihood of a serious breach.

In the longer-term, more SecOps team members calling in sick or leaving the profession altogether leaves the remaining ones with an even greater workload, creating a vicious cycle of stress, under-staffing, and risk exposure. It will also lead to fewer younger recruits: when choosing roles, Gen Z-ers are more likely to prioritise work-life balance and personal wellbeing than traditional factors like income.

What effect has the increased pressure had on you?



41%

said they have had to seek help for work-related stress due to issues such as migraines, panic attacks or high blood pressure.

VIEW FROM VECTRA

Steve Cottrell, EMEA CTO on creating a healthier security environment

As odd is it may sound, the pressure on security leaders rarely comes from the external threat landscape and trying to detect and respond to attacks. The pressure actually comes from internal politics. The CISO often has to be the conscience of the organisation when individual business leaders prioritise the capability they need over the risk to the organisation as a whole, or the security needs of the customers.

The CISO often has to be the conscience of the organisation when individual business leaders prioritise the capability they need over the risk to the organisation as a whole, or the security needs of the customers.

After a breach, security teams may face heavy scrutiny. But security leaders shouldn't always take the blame. In most cases, CISOs will have requested budget, assets and changes that weren't signed off – they must be ready to remind the board that security is a shared responsibility.

Reporting lines into the CIO or CTO tend to increase stress levels too, as there is an inherent conflict. CISOs are incentivised on managing risk and reducing the chances of a breach, whereas CIOs are judged on the speed of delivery, capabilities delivered, and cost. It's not hard to see that the two agendas can oppose each other. So, opening up the lines of communication, being able to measure the success of security and ensuring that everyone is bought in to security will help to ease some tensions. After all, we are all on the same team.

Regardless, these stats should be a wake-up call. Security teams and their leaders need support to shift away from the constant cycle of over-working and anxiety. With an improved focus on workforce wellbeing, increased investment, better training, and the right tooling, we can start turning the tide.

Fortunately, there are resources that organisations can turn to for support in managing team wellbeing. The charity, Mind, has a list of useful resources to help combat workplace stress: from improving work-life balance and better managing workload, to building resilience through mindfulness, physical exercise and other activities.

For more sector-specific guidance, industry association CREST has compiled a detailed report based around first-hand experiences and workshop discussions. It's designed to provide help for employees and employers alike—including how to recognise the tell-tale signs of stress in oneself and others.

Finally, there's Dr Ryan Louie, founder of the Psybersecurity Clinic and a passionate advocate of mental health awareness in the industry. His website lists previous presentations on the subject, and a handy list of recommended further reading.

Conclusion

Security teams are increasingly overwhelmed by workplace stress. It's driven in part by more determined and better resourced threat actors, and more complex and harder-to-protect IT environments. But that's not the whole story. Staff shortages and resource constraints are having an outsized impact on their ability to perform effectively at work.

Given what is at stake, organisations must act now. This is not about eradicating workplace stress. Dealing with a live attack is a high-pressure event and one in which a certain amount of stress can actually motivate teams. But when anxiety and workload become excessive, things can quickly slip into a downward spiral.

So, what's the answer? Based on our discussions with and feedback from all levels of the security organisation, here are our top 3 recommendations:

1. **Use a threat-led model to clarify priorities**. Continuous firefighting plays a prominent role in the burn-out within security teams. Using a threat model to define a clear strategy and priorities can help in shifting from reactive to proactive and bringing teams a better sense of focus, control, and achievement.
2. **Invest in automation**. Grunt work makes security teams feel undervalued, and to move on to new positions in search of a better experience. Automating this low-value work – whether that means automating ticket-enrichment workflows or applying AI/ML to find and prioritise threats—will pay dividends in a happier and more engaged team.
3. **Lead a cultural change in the organisation**. Too many organisations view security as the sole responsibility of the CISO. One of the hardest but most crucial changes that a CISO can effect is to shift that mentality and make every member of staff a "security professional", invested in the benefits of doing it well and consequences of doing it poorly. This repositions the security team in a more strategic and positive light, brings earlier engagement in business initiatives, and leads to better security outcomes…that don't require yet more firefighting.

Staff shortages and resource constraints are having an outsized impact on their ability to perform effectively at work.

VECTRA
SECURITY THAT THINKS

How Vectra can help

This is where Vectra comes in. Vectra helps organisations to stay out of the headlines by disrupting attackers before they can cause harm. Vectra is the leader in threat detection and response – from cloud and data centre workloads to user and IoT devices.

Vectra takes a modern, AI-driven cloud security approach to threat detection and response, providing vital security context – delivering timely and meaningful threat assessments to prioritise events. The Vectra platform accelerates threat detection and investigation, using AI to enrich the network metadata it collects and stores with the right context.

In this way, Vectra acts like an extra member of the SecOps team, researching and analysing threats 24/7 to give human engineers the information they need to neutralise threats in real-time. In short, Vectra takes the pressure off the SOC and helps to keep the organisation safe.

See threats. Stop breaches.

Request a Demo

Email info@vectra.ai vectra.ai

Version **040422**