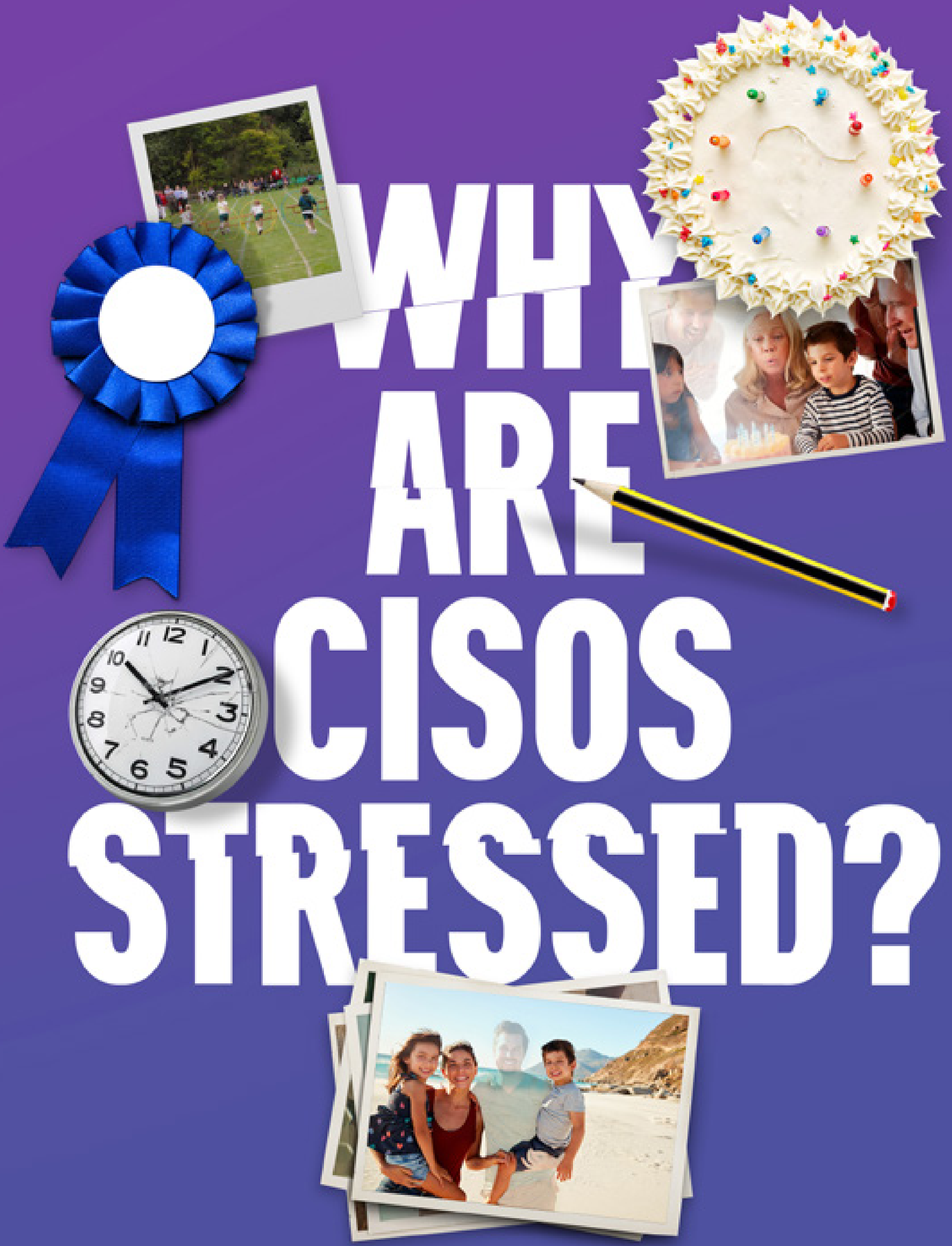
NOMINET
CYBER
SECURITY

CISO STRESS

Life Inside the Perimeter: One Year On



THE CISO STRESS REPORT

Life Inside the Perimeter: One Year On

EXECUTIVE SUMMARY

Foreword: Russell Haworth, CEO, Nominet

The "human factor" has become a key discussion point in the cyber security community. In an industry that has historically arguably focused more on tech than people, the humans behind both threats and security have been sorely overlooked. Even the CISO, the conductor at the head of every security team, has been an elusive figure.

At the beginning of 2019, we undertook a research project to rectify this. We sought to better understand the CISO – their role, their pain-points, what keeps them up at night. This first report, *Life Inside the Perimeter* revealed the position to be a uniquely difficult role, and that the average CISO was under high levels of stress that were impacting their welfare.

Over the past 12 months we have been told countless times by CISOs and security professionals that this research resonated with them and their personal experiences. Having to balance the responsibility for fighting increasingly sophisticated threats and communicating their business case effectively to the board, has put them under strain.

We quickly identified that the missing piece of the puzzle was the board's perspective – how did they view the CISO, the security team and cyber security as a wider business issue? We commissioned a second piece of research to find answers to these questions. The resulting report, *Trouble at the Top* confirmed that the board in many organizations had not got to grip with the issue of cyber security, and had not empowered their CISO to help them.

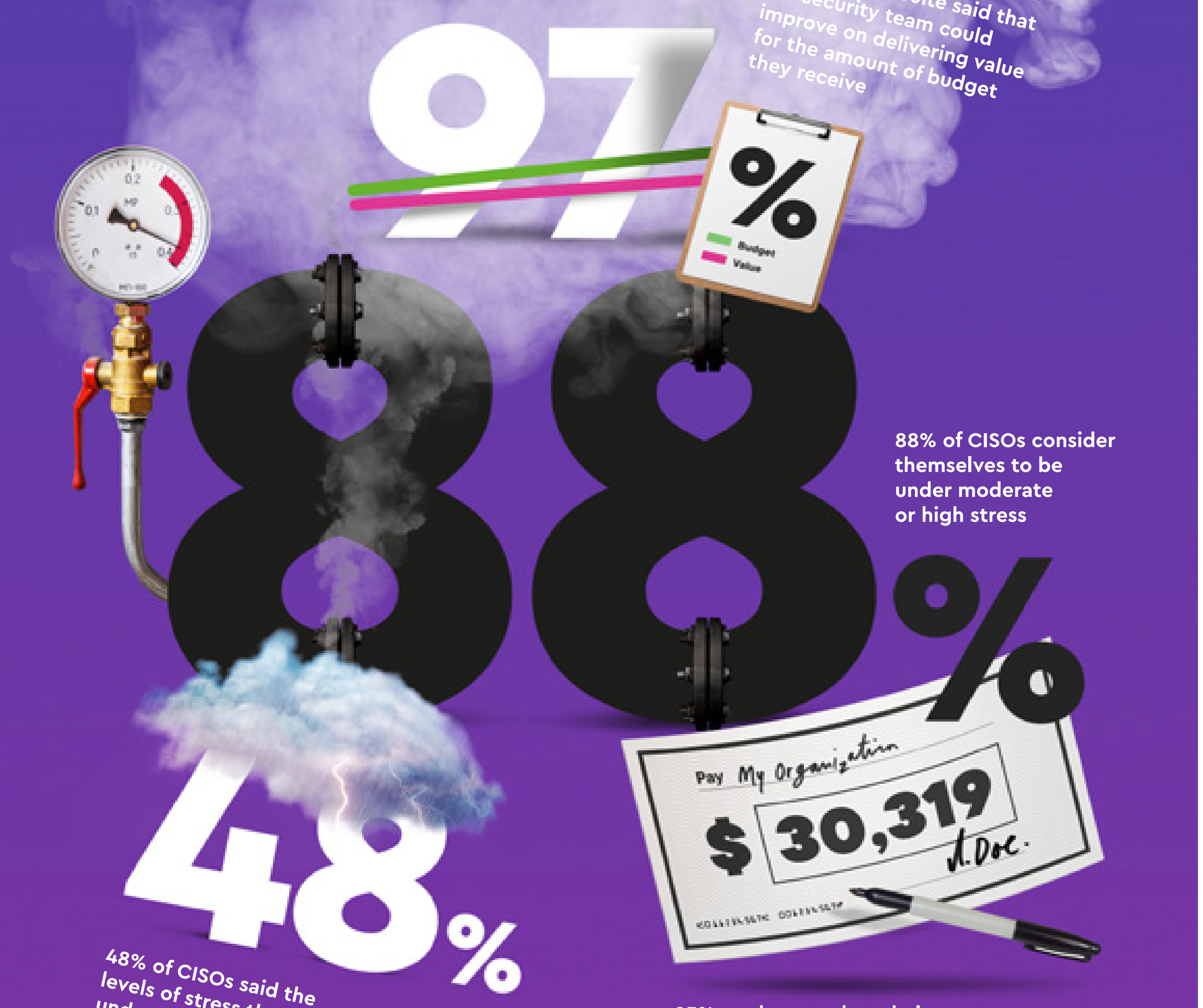
Having identified these issues, this year's report aims to check in on the CISO a year on and – using last year's results as a benchmark – gauge how and if the CISO's role has improved. However, raising awareness of the pressures CISOs are under is only half of the job. This year we also looked to go further, drilling down into the causes to identify where stress could be alleviated.

We have also simultaneously surveyed the board, asking them complementary questions to qualify their perspective on the role of the CISO. This allows us to identify certain aspects of the CISO's role where the opinion of the C-Suite and CISO diverge. These divergences expose pain-points, where the C-Suite and CISO are no longer working in tandem and are arguably pulling in different directions.

The objective is to uncover these points of misunderstanding, misinterpretation or conflict in order to build a more productive relationship between the board and CISOs. We believe that fostering mutual support and understanding between the two is the most impactful way of materially improving the working life of the CISO.

What's more, from the board's perspective, an improved relationship with the CISO is more likely to help them retain staff, catch attacks earlier, improve business readiness and response and minimize damage. It will also give the board a better appreciation for the security risk the organization is facing and what is needed to build a more defensible and stable environment.

While we hoped that the job of the CISO had improved in the past year, it's simply not the case. We are potentially heading towards a burnout crisis if the very people who we are relying on to keep businesses secure are operating under mounting pressure. CISO stress is on the rise – with almost 90% moderately or tremendously affected – and it's taking a greater toll on their personal lives and well-being. Not only is this harming the lives of CISOs but it will ultimately make it harder to retain staff, catch attacks early and improve security. It is worrying that at board level, understanding of these pressures appears not to have translated into action.



97% of the C-Suite said that the security team could improve on delivering value for the amount of budget they receive

88% of CISOs consider themselves to be under moderate or high stress

48% of CISOs said the levels of stress they are under has impacted their mental health

95% work more than their contracted hours – CISOs are giving organizations $30,319 (£23,503) worth of extra time per year

METHODOLOGY

In autumn 2019, Nominet commissioned Vanson Bourne to conduct 800 online surveys with C-Suite executives and Chief Information Security Officers (CISOs) in the US and UK.

Respondents all worked at organizations with 3,000 or more employees, across a range of public and private sectors. C-Suite executives were all members of the board.

400 surveys were achieved for each job role split (C-Suite and CISO), with six extra CISO respondents included, all of whom were recommended to participate via Nominet.

1. CISO stress levels remain high

The vast majority of CISOs remain moderately or tremendously stressed. This report shows that this stress is now taking a greater toll on CISOs' mental and physical health, and their personal relationships. This also has negative effects for organizations, as it has a measurable impact on the CISO's ability to execute their role and results in burnout, with the average tenure of a CISO being just 26 months.

2. Poor work-life balance is a key contributor to stress

Almost all CISOs are working beyond their contracted hours, on average by 10 hours per week. Even when they are not at work, they are unable to switch off, and this means their personal lives are disrupted. CISOs reported missing family birthdays, vacations, weddings and even funerals. They're also not taking their annual leave, sick days or time for medical appointments – contributing to physical and mental health problems.

3. C-Suite understanding is improving but action is not forthcoming

The board's understanding of cyber security is increasing. They grasp the risk it poses to their organization, they know it could cost them their job, and they even recognize that the CISO is under a lot of stress. However, they consistently underestimate the impact that stress and long-hours are having on the CISO and – in fact – want the CISO to deliver more value to the business. This burden of responsibility and a perceived lack of support from the board is also a key contributor to CISO stress.

CISO STRESS TEST

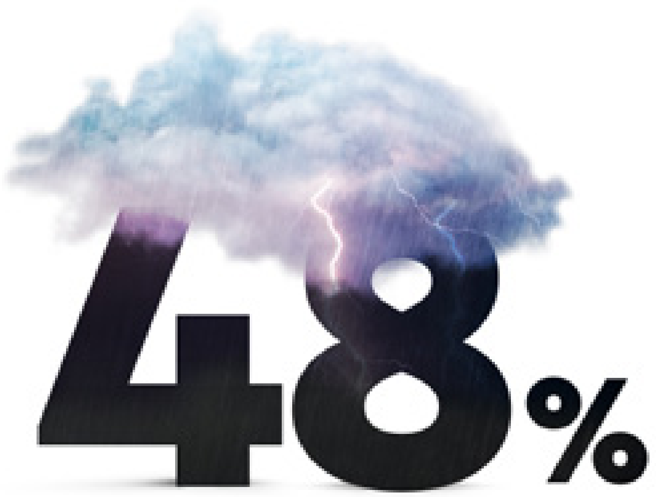
STRESS LEVELS & IMPACT

The most significant discovery from our research last year was just how much stress the average CISO is under. Unfortunately, this remains a common component of the CISO role 12 months on. Still, 88% of CISOs consider themselves to be under moderate or high stress, only slightly down from 91% last year. This 3% decrease can hardly be considered an improvement.

Even more concerning, these consistently high levels of stress seem to be taking a greater toll on the welfare of CISOs. Almost half (48%) reported that the levels of stress they are under has impacted their mental health. While the numbers are close, US respondents reported more stress-related mental health issues.

The percentage of CISOs believing that stress levels are affecting their mental health is almost twice as high as last year (27%). The reason behind this increase isn't much of a mystery. Sustained levels of high stress in the workplace are clearly taking their toll. Many CISOs also reported that their stress had impacted their physical health.

Have your stress levels affected your mental health?



48% of CISOs said the levels of stress they are under has impacted their mental health

Of course, as the CISO plays such a critical role, their stress also has an impact on the business. Almost a third (31%) of CISOs said stress had affected their ability to do their job. As with last year, the research also exposed high staff turnover of senior security personnel, with both CISOs and the C-Suite saying the average tenure of a CISO is just over two years (26 months). It is therefore in the interests of the entire business to get to the root of the problem of CISO stress and to alleviate it.

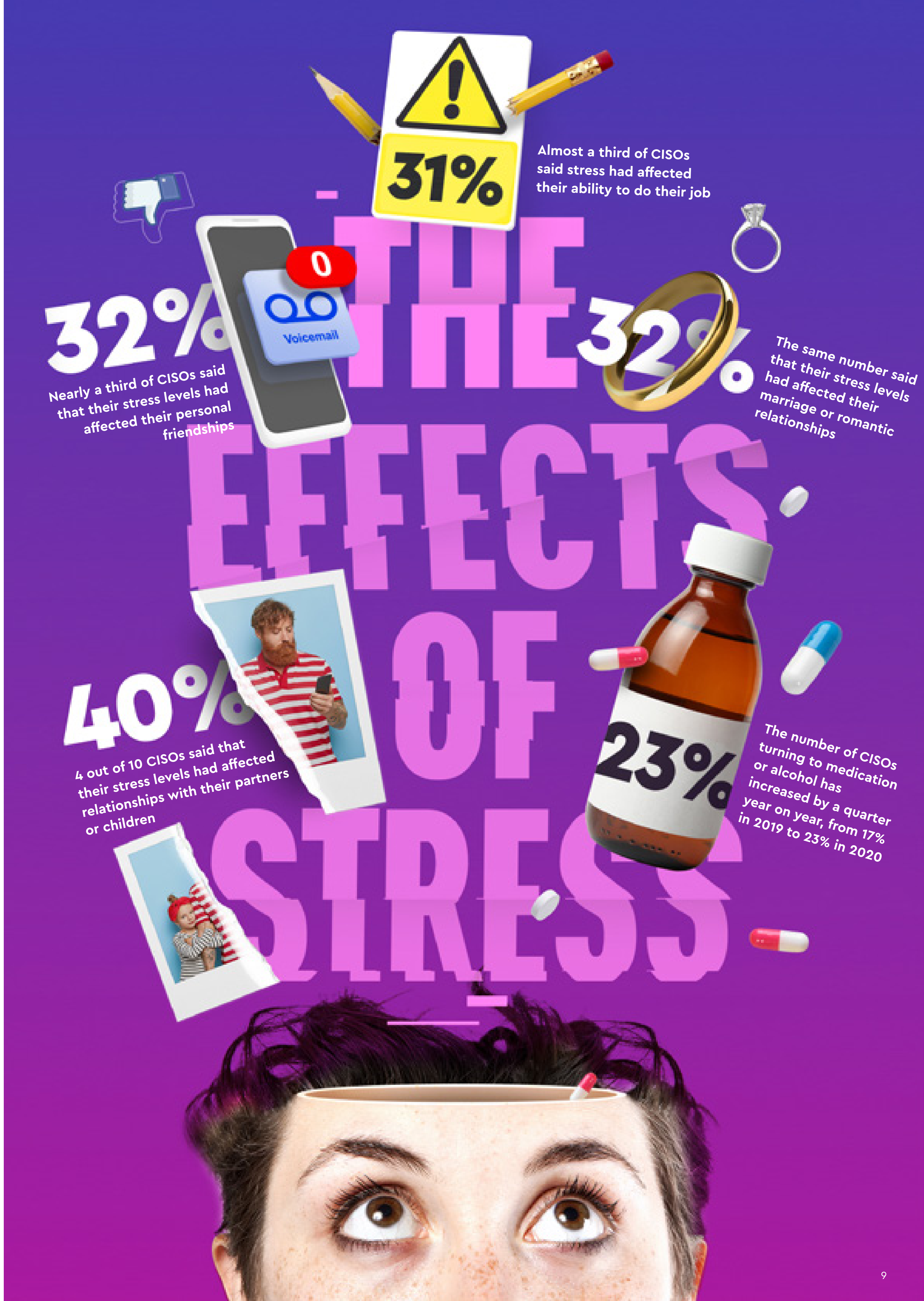
35% of CISOs reported that their stress had impacted their physical health

EFFECT ON PERSONAL LIFE

Once again, our research found that an alarming number of CISOs (23%) are turning to medication or alcohol to manage their stress (up from 17% last year). UK respondents were slightly more likely to self-medicate than US respondents (25% vs. 20%)

However, this year we wanted to delve deeper into the impact work-related stress is having on the personal lives of CISOs:

- 40% said that their stress levels had affected their relationships with their family or children
- 32% said that their stress levels had affected their marriage or romantic relationships
- 32% said that their stress levels had affected their personal friendships



Almost a third of CISOs said stress had affected their ability to do their job

Nearly a third of CISOs said that their stress levels had affected their personal friendships

The same number said that their stress levels had affected their marriage or romantic relationships

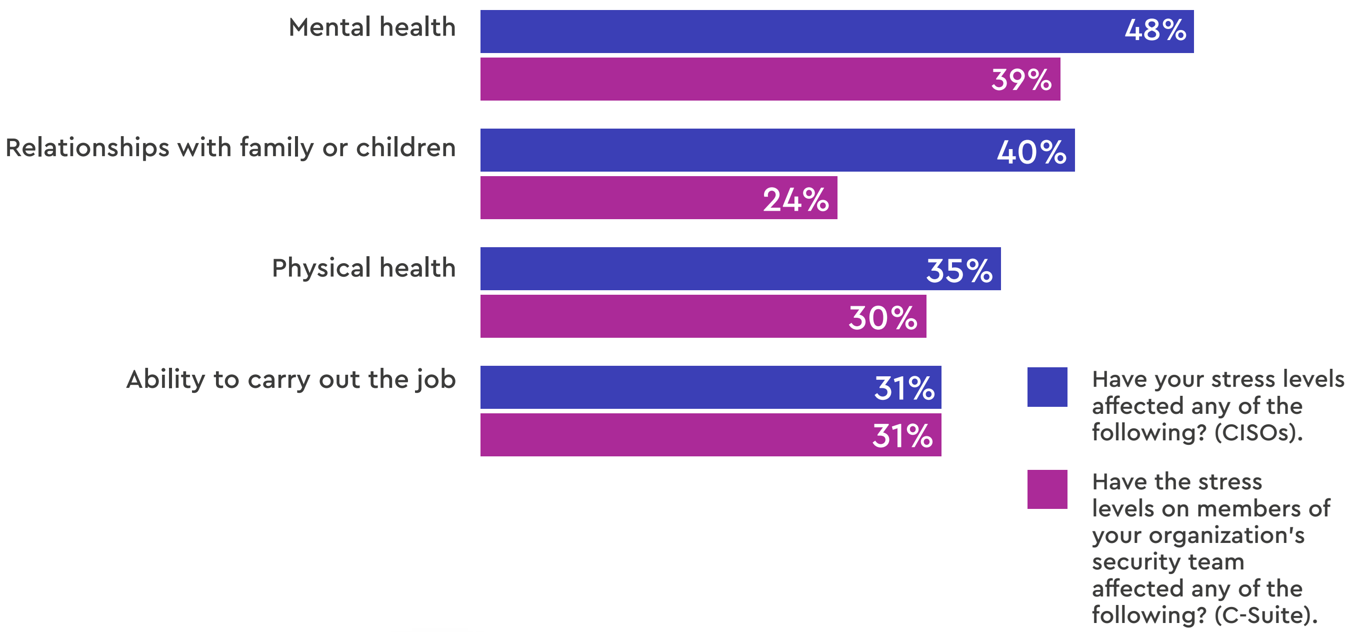
4 out of 10 CISOs said that their stress levels had affected relationships with their partners or children

The number of CISOs turning to medication or alcohol has increased by a quarter year on year, from 17% in 2019 to 23% in 2020

WHAT THE BOARD THINKS

The high-pressure nature of the CISO's job isn't totally lost on the C-Suite, with 74% saying they believe their security team to be moderately or tremendously stressed. However, boards consistently underestimate the personal impact of workplace stress on their security team.

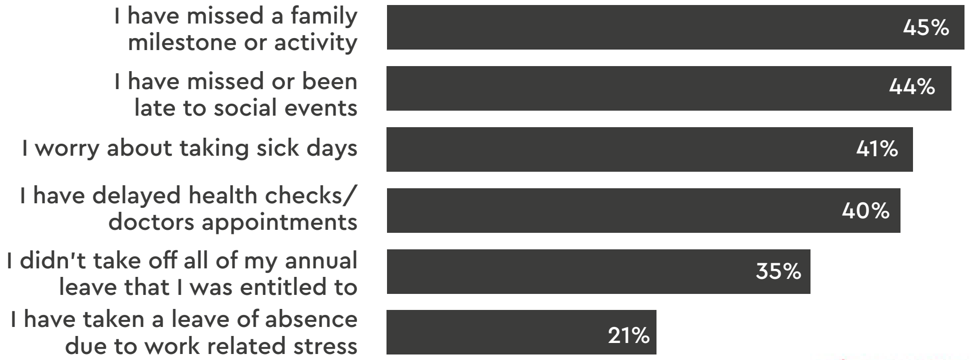
The only thing both CISO and C-Suite respondents are both agreed on is the rate at which stress is impacting the CISO's ability to do their job. It's interesting that this should be the only area of a CISO's life where the C-Suite haven't underestimated the effect of stress, probably because this is where they can see the impact first-hand and because it also impacts them.



Gary Foote, CIO
Haas F1 Team

> "I'm not surprised to see that stress levels are consistently high from 2019 to 2020, with the threat landscape continuously shifting. But it is always disappointing to read that it continues to have a big impact on the personal lives of my peers. Mental and physical health at work is a hugely important subject, and though some organizations are recognizing this and reacting positively, there is still a lot of progress to be made. Burnout will neither help the CISOs, the board or the business, and consequently accelerated change is required to ensure security teams are supported; technically, financially and personally."

Which of the following have you done/not done as a result of work commitments in the last year?

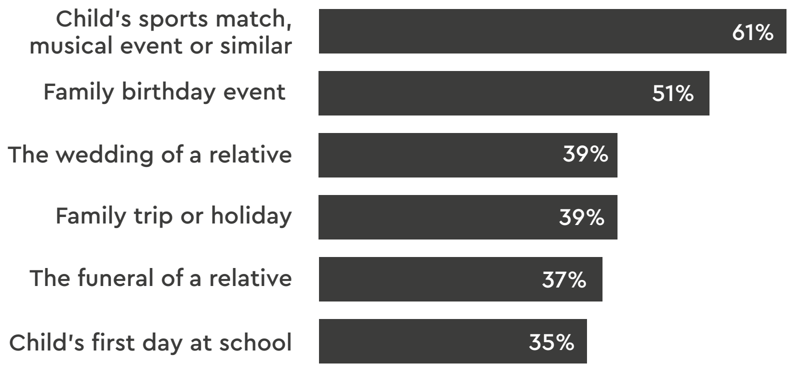


39% of CISOs who have missed a family milestone or activity have missed a family wedding due to work commitments

Almost all CISOs are working beyond thier contracted hours, on average by 10 hours per week

Which of the following family milestones or activities have you missed in the last year as a result of work commitments?

(Of those who have missed a family milestone or activity)



WHAT DO THE EXPERTS HAVE TO SAY?

Dr Dimitrios Tsivrikos, Lecturer in Consumer and Business Psychology, University College London

"Given the unstable political, social and technological challenges that we are facing in the new decade, it is unsurprising to see that individuals working in this sector (CISOs) are incredibly stressed. This is very much in line with key psychological findings concerning people working in the security and technology sector and, most likely, we anticipate that these individuals will be reporting some of the highest levels of stress within the industry.

"While there have been positive steps in mental health and stress-related issues, the essence of tackling these issues has not received as much attention as needed. While measuring, understanding and incorporating key findings within the work is incredibly important, we also need to consider that there is a lack of research that looks into the work-life balance.

"Indeed, work-life balance is one of the key components that may contribute to work stress, and a closer look into lifestyle choices, and realizing that people in this industry can provide a great insight will help us to understand how we can support such individuals.

"We do anticipate that stress levels will continue to rise until we address the issue of stress, mental health and well-being at work. These are issues that are recognized but we have to match awareness with passion for actually tackling stress and allowing employees to live a happier and healthier life. Please find below the top techniques of how to reduce stress in the workplace."

HOW EMPLOYEES CAN ALLEVIATE WORK STRESS:

- Maintain a positive social life – develop good supportive relationships
- Exercise – releases endorphins (happy hormones)
- Maintain a balance between work life and personal life
- Take control of your stress
- Avoid unhealthy habits e.g. poor diets
- Try to be positive – "try to be glass half full instead of glass half empty"

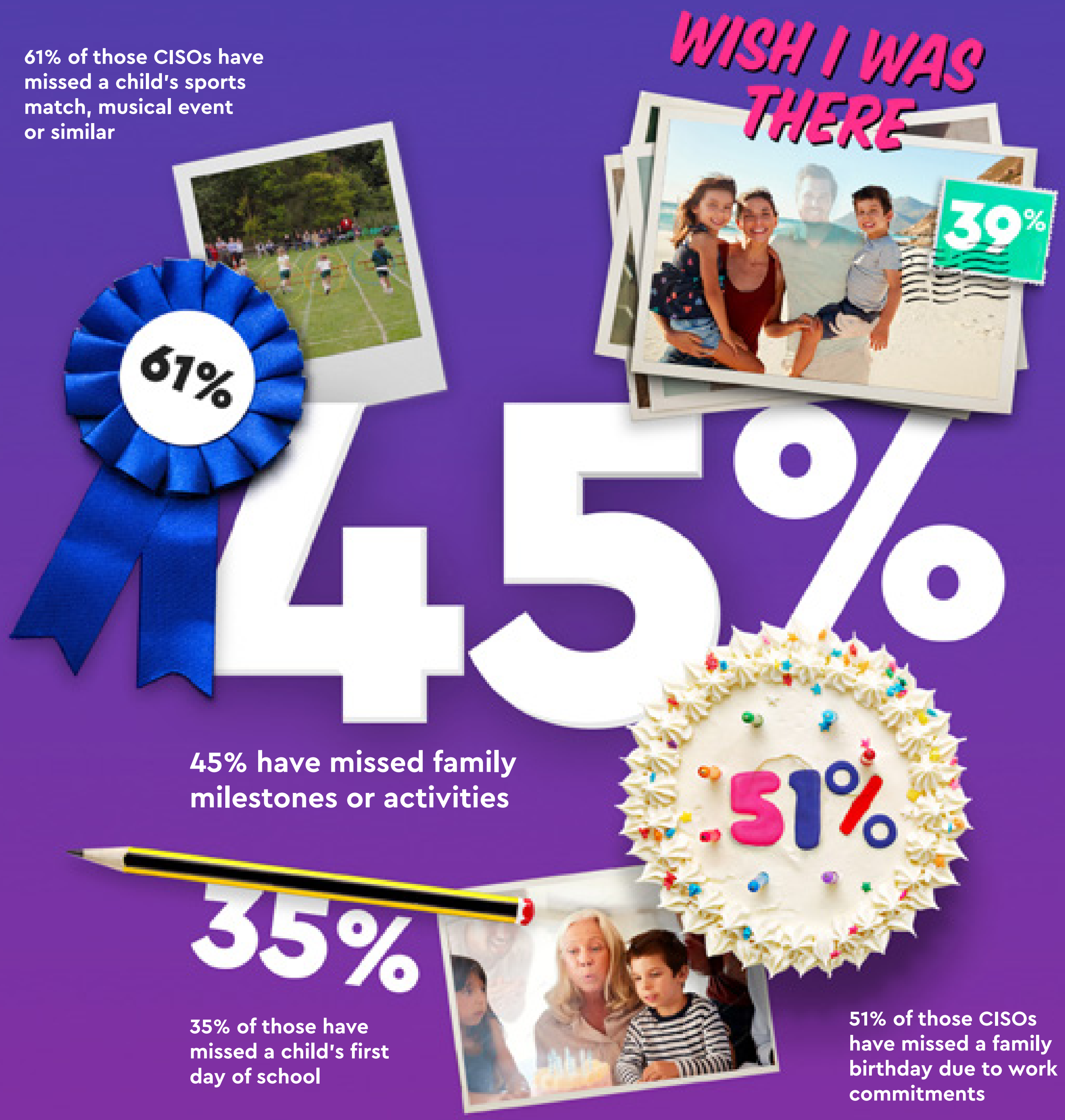
References:

D. LaMontagne A., Keegel T.V.D., (2007) Protecting and promoting mental health in the workplace: developing a systems approach to job stress. Health Promotion Journal of Australia 18, 221–228.

Leka, S., Griffiths, A., Cox, T., & World Health Organization. (2003). Work organisation and stress: systematic problem approaches for employers, managers and trade union representatives. World Health Organization.

Work-life balance. Retrieved 16 January 2020, from https://www.mentalhealth.org.uk/a-to-z/w/work-life-balance

2018 BDO Cyber Governance Survey. (2018). Retrieved 16 January 2020, from https://www.bdo.com/insights/assurance/corporate governance/2018-bdo-cyber-governance-survey-board-perspecti



39% of those have canceled a family trip due to work commitments

61% of those CISOs have missed a child's sports match, musical event or similar

45% have missed family milestones or activities

35% of those have missed a child's first day of school

51% of those CISOs have missed a family birthday due to work commitments

71% of CISOs said their work-life balance is too heavily weighted towards work

DRIVERS OF CISO STRESS

WORK-LIFE BALANCE

Faced with evidence that CISO stress remains high, it is important to interrogate the causes. First, we looked at the work-life balance of the CISO, and how this could be contributing to their stress. A large percentage of CISOs (39%) said that they found long hours to be one of the most stress inducing parts of their job.

It was clear from the research that the work-life balance of the average CISO is too heavily weighted towards work. Working hours are increasing for CISOs, with 95% working more than their contracted hours – on average, 10 hours longer. 59% of CISOs worked 10 hours or more above their contracted hours a week, a big increase on 34% last year.

Furthermore, even when they are technically out of the office, only 2% of CISOs said they were always able to switch off, with the vast majority (83%) reporting that they spend half their evenings and weekends or more thinking about work.

What is particularly concerning is that 87% of CISOs say that working additional hours was expected by their organization. Largely, the C-Suite agree – 78% admitted that they expect the security team to work beyond their contracted hours. Expectations for longer hours were reported to be higher in the US, although the hours the CISO works overall were comparable.

US VS UK

Q We asked CISOs, is it expected that you/the wider security team in your organization work longer hours than you/they are contracted for?

🇺🇸	Yes 90% No 10%	🇬🇧	Yes 82% No 18%

Q We asked CISOs, do you work extra hours beyond your contract (based on a 40-hour working week as standard)?

🇺🇸	Yes 94% Av. 10 hrs extra	🇬🇧	Yes 95% Av. 9 hrs extra

Q We asked the C-Suite, is it expected that the security team In your organization work longer hours than they are contracted for?

🇺🇸	Yes 83% No 17%	🇬🇧	Yes 73% No 27%

MONEY TALKS

It's difficult to put tangible figures on subjects like personal stress and work-life balance – but cash is one way to do it.

With the data showing that an average CISO's wage is $121,277 (£94,013)[1] – and that they are working 10 hours extra a week – organizations are getting an average of $30,319 (£23,503) per year in free CISO time.

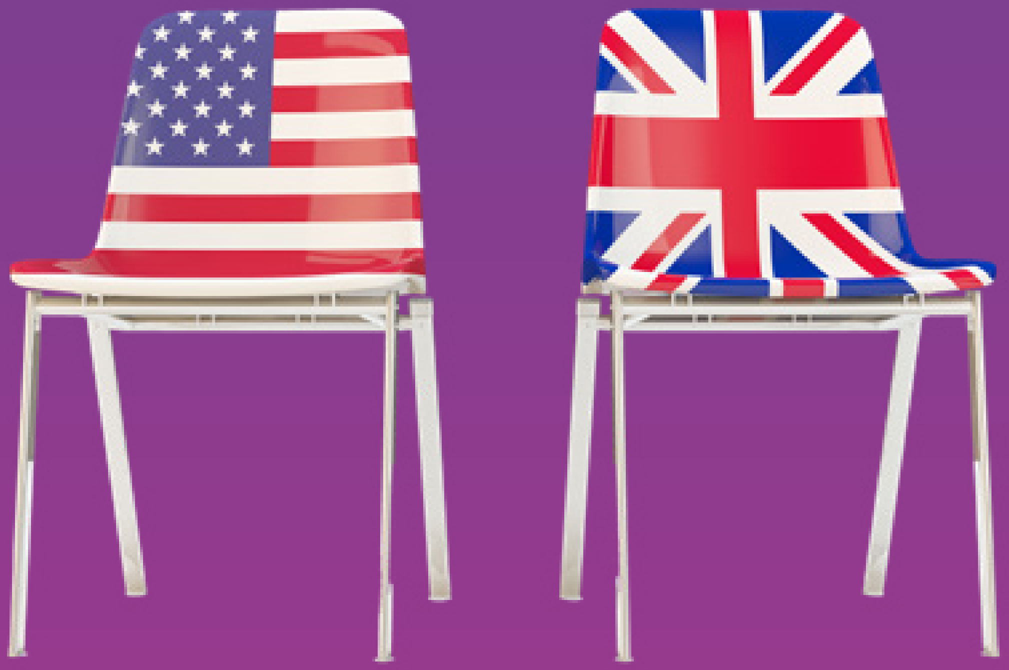
Revealingly, almost all surveyed CISOs (90%) said they'd take a pay cut if it improved their work-life balance. On average, CISOs said they'd be willing to give up 7.76% of their wage, which equates to $9,642 (£7,475) per year.

The average American CISO

- Wage $128,908
- Gives their organization $32,227 of unpaid work a year
- Would sacrifice $9,596 a year for a better work-life balance

The average British CISO

- Wage £88,324
- Gives their organization £19,873 of unpaid work a year
- Would sacrifice £7,509 a year for a better work-life balance



[1] All conversions based on exchange rate on 10/27/2019. £1 : $1.29

90% of CISOs said they'd take a pay cut if it improved their work-life balance

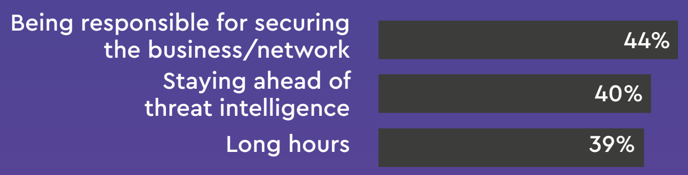
A fifth of CISOs believe they themselves would be fired whether they were responsible or not for a breach

RESPONSIBILITY FOR A SECURITY BREACH

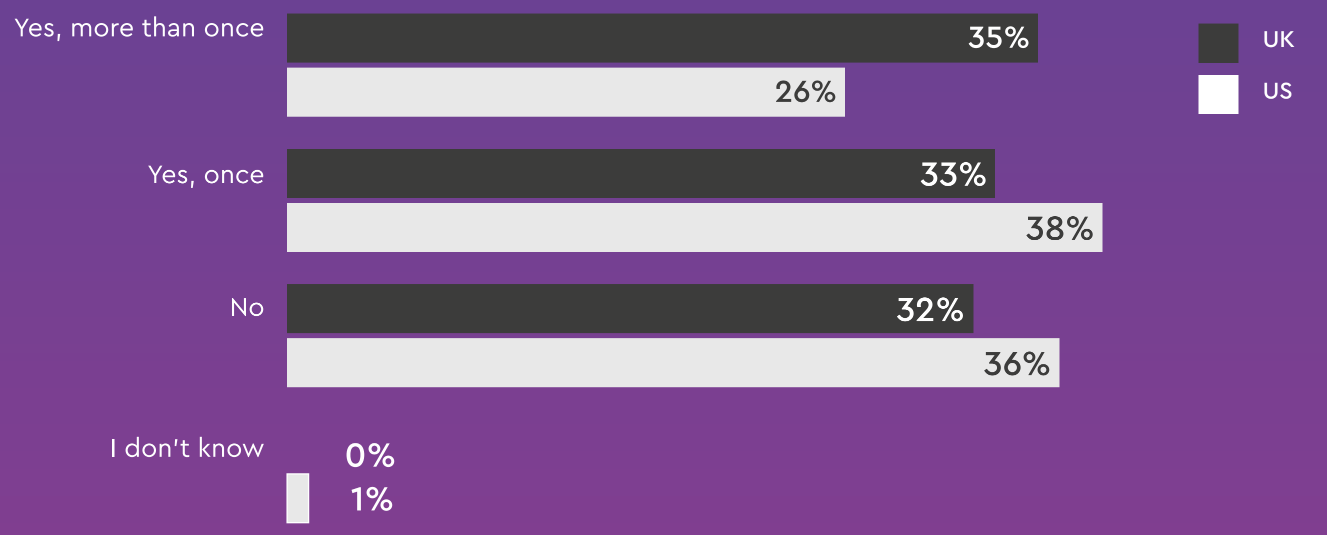
When asked to identify the most stressful parts of the job, CISOs ranked the responsibility of securing the business/network as the highest, slightly ahead of the long hours.

As the rate of cyber crime shows no sign of slowing, this stress is being compounded by the increasing regularity of cyber incidents. According to the responses from CISOs and the C-Suite, 66% of the organizations surveyed have experienced at least one security breach in the past year, with 30% saying they had experienced multiple.

What are the most stress-inducing parts of the job?



Has your organization been affected by a security breach in the past 12 months?



However, as much as the threat of cyber crime is in itself, the key part of the stress may in fact be the CISO's perception that they are responsible if their company is breached. 37% of CISOs and 31% of C-Suite believe the CISO is ultimately responsible for the response to a security breach.

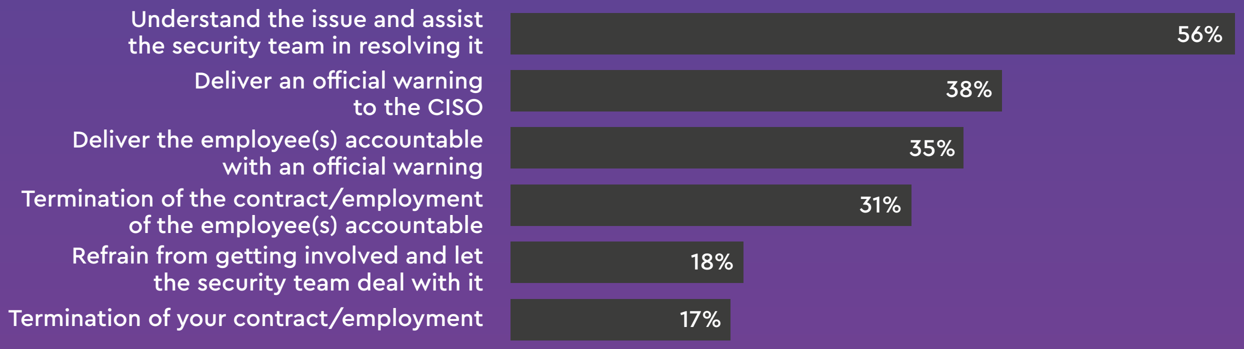
This is particularly worrying when you take a look at NCSC guidance around board responsibility for cyber. The NCSC says that due to cyber being so critical to ensuring that organizations can exploit the opportunities that technology brings, it "places it firmly within the responsibility of the Board'.[2]

[2] Source: National Cyber Security Centre. ncsc.gov.uk/collection/board-toolkit/implementing-effective-cyber-security-measures

Furthermore, while it is generally accepted in the security community that a breach is inevitable, this is evidently not accepted on every board. Nearly a quarter (24%) of CISOs said that their board doesn't accept that breaches are inevitable. That view is confirmed by C-Suite respondents, with 24% saying they don't view breaches as inevitable and a further 10% admitting they don't know.

When there is a security breach, the stakes are high for the CISO. 29% of CISOs believe that the executive team would fire the responsible party, which is confirmed by the C-Suite (31%). A fifth (20%) of CISOs believe they themselves would be fired whether they were responsible or not, which is a considerable increase on just 8% last year. Interestingly, 17% of C-Suite believe they themselves would be fired.

How would your organization be likely to respond in the event of a significant security breach? (C-Suite)



21% of CISOs believe there to be no support structures in place within their organization to help them deal with stress

A LACK OF C-SUITE SUPPORT?

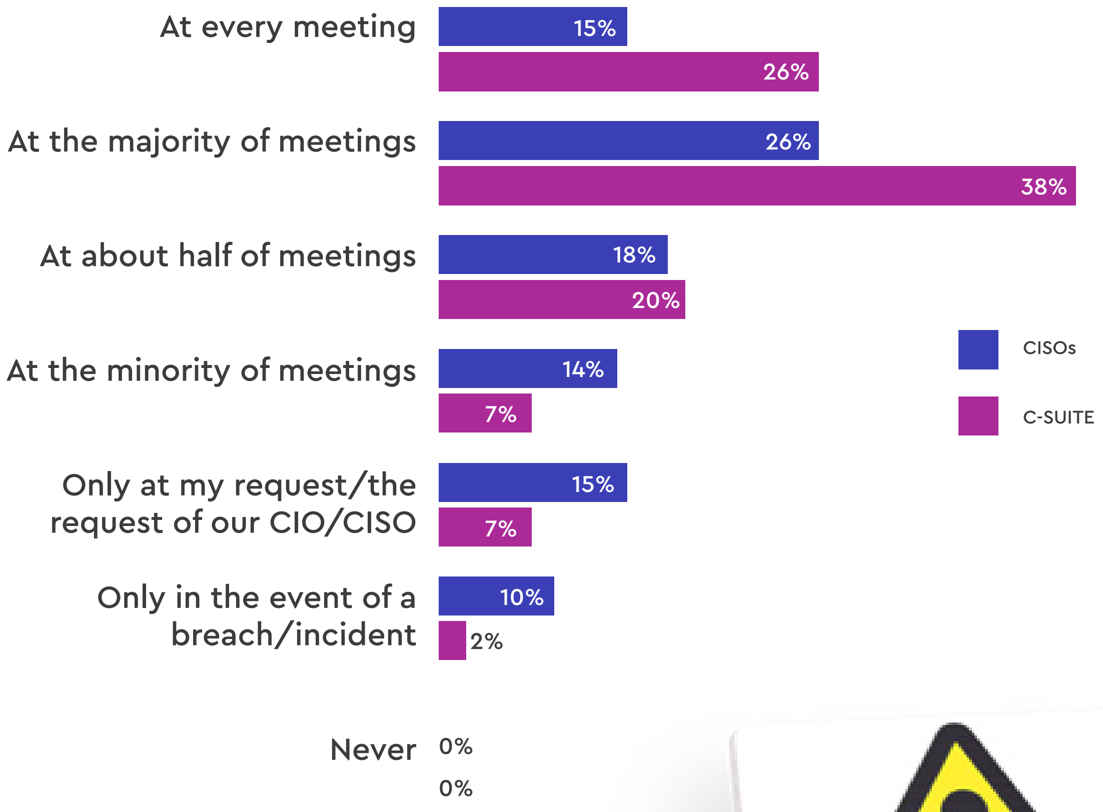
The burden of responsibility felt by the CISO is undoubtedly worsened by a perceived lack of support from the board. However, this is where the CISO and C-Suite disagree most.

39% of CISOs believe that cyber security is an official agenda item for board meetings less than half the time. A quarter reported that it only became a board issue on their request or in the event of a security breach or incident, suggesting that the treatment of security is very reactive.

The C-Suite sang a different tune, with a massive 84% saying that it was an official agenda item on half or more boardroom meetings, with 26% claiming that it was on the agenda of every board meeting.

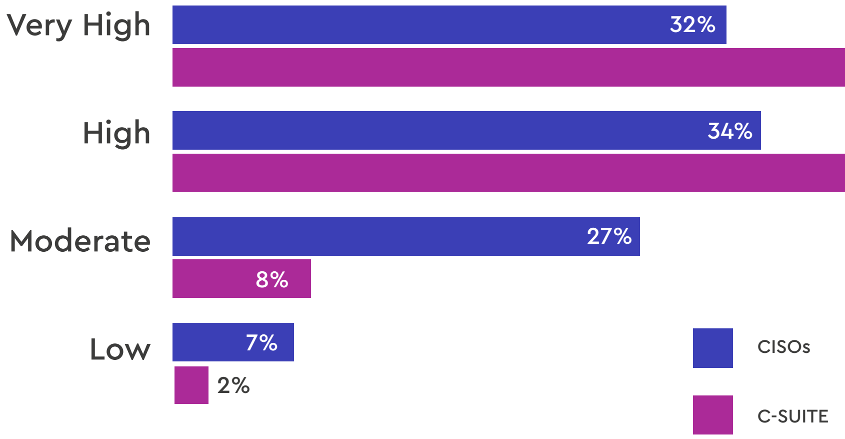
However, it would be wrong to assume that the C-Suite doesn't take security seriously, as 47% of the C-Suite say cyber security is a "great" concern to them. They are actually more likely than CISOs to think that cyber threats are a "high" or "very high" risk to their business (90% vs 66%).

How regularly is cyber security an official agenda item at board meetings in your organization?



47% of the C-Suite say cyber security is a 'great' concern to them

How much of a risk do you consider cyber threats to be to your organization?



"The responsibility of cyber crime has never weighed so heavy; on the board and on the CISO. With increasingly sophisticated cyber threats posing a greater risk – whether that be to organizations, consumers or critical national infrastructure – there is a lot at stake."

"As this contextual environment evolves it will become increasingly important for CISOs and the board to have open and clear conversations about risk, threats and defense. The CISO will need to become a bridge between technical teams and business leaders, to ensure that priorities are understood, expectations are reasonable, and remediation can be fast."

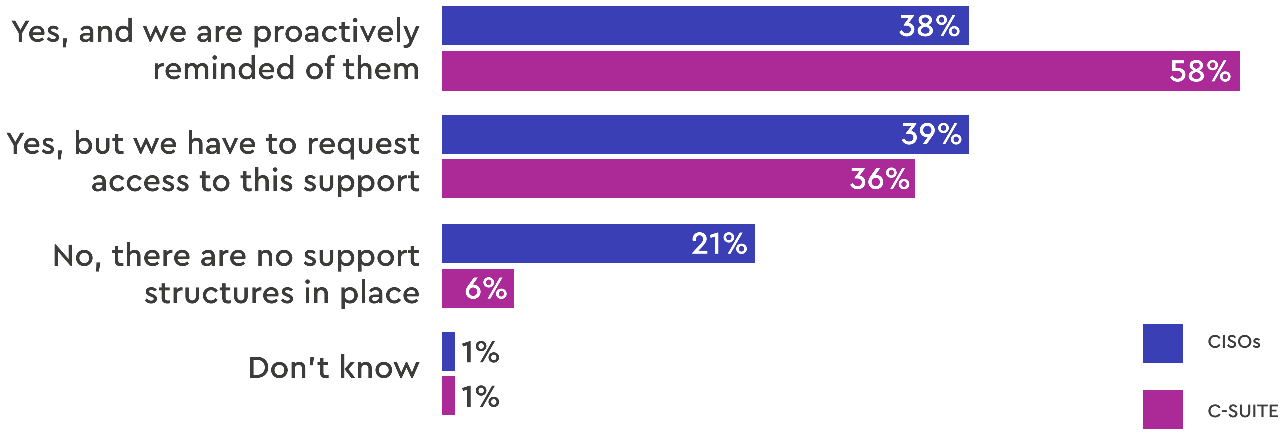
Russell Haworth, CEO Nominet

Is the real issue that the board lacks personal support for CISOs?

This belief is laid bare when it comes to the issue of support for mental health problems which, as we have discovered, affects many CISOs.

When asked if there were support structures in place to help deal with stress, one in five (21%) of CISOs said there were none in their organization. The C-Suite disagrees, with 94% claiming that there are, although even 36% of the board admitted that CISOs weren't proactively reminded of them, and that the security team would have to request access for support.

Does your organization have support structures in place to help you or any other employees with the stresses of your/their job?



97% of the C-Suite said that the security team could improve on delivering value for the amount of budget they receive

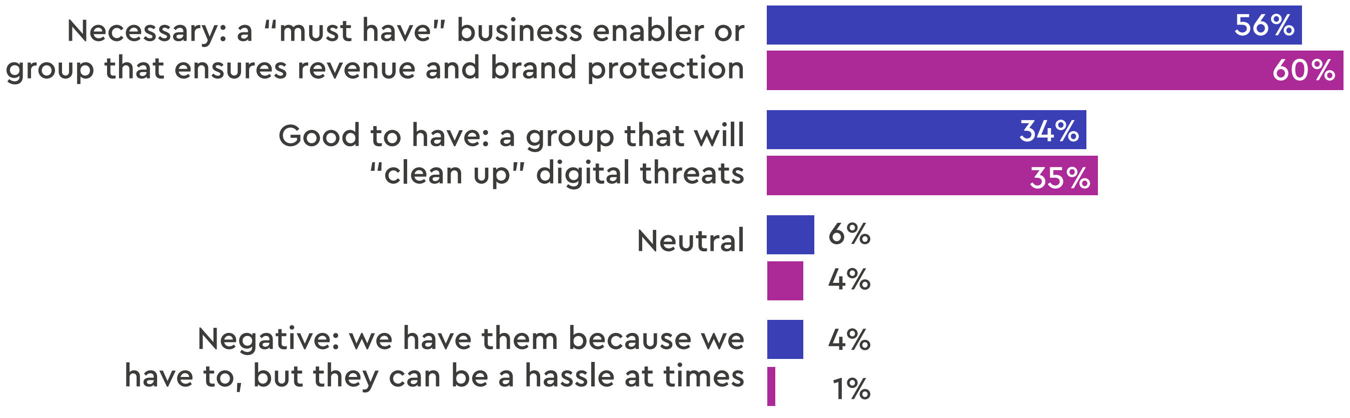
THE BOARD THINKS THE SECURITY TEAM COULD BE DOING MORE

While there is some disparity in responses, the research demonstrates that the board do in fact have a relatively good understanding of the CISO's difficult position – from the risk of cyber crime to an acknowledgement of the stress CISOs are under. However, some of the most alarming results show that, in spite of that, the C-Suite still expect more from the CISO.

Almost all of the C-Suite respondents (97%) said that the security team could improve on delivering value for the amount of budget they receive. This suggests that, despite how much effort the CISO puts in, business leaders still think they should be getting more.

The issue may well reside in how CISOs are communicating their value to the board. Again, almost all C-Suite respondents (94%) said that the CISO could do a better job at demonstrating their value. Indeed, 29% of CISOs said dealing with the board is one of the most stress-inducing parts of the job.

Arguably this comes down to a misconception of the CISO's role and what value they can bring. When asked how they view their organization's security team, 60% recognized they were necessary, but still more than a third (35%) viewed them as a "good to have: a group that will clean up digital threats". Unfortunately, 34% of CISOs accurately predicted that this is how the board sees them. This speaks to a fundamental lack of understanding and appreciation of the strategic role a CISO should play within a business.



🟦 CISOs: How do you think the executive management (business/non-technical) and board of directors at your organization views the security team?

🟪 C-SUITE: How do you view your organization's security team?

CONCLUSION

The main learning from this report is that the work life of the CISO has not materially improved over the past year. In fact, consistent levels of high stress are becoming a greater burden on the CISO's wellbeing and personal life. Until this stress is relieved, the CISO's ability to deliver value to the business will be diminished as their ability to do their job is hampered and they quickly become burnt out.

The role of the CISO can only be improved by a better working relationship with the board. The causes of CISO stress – poor work-life balance, overbearing responsibility for security breaches, and a lack of support – are within the C-Suite's power to change.

The first step is to raise awareness of the challenges facing CISOs, the stress that they are under and the highly complex task of protecting an organization's most valuable assets. Largely, the research suggests that progress has been made in this regard. The board do understand the risk of cyber crime to their organization and they even appreciate that the CISO is placed under considerable stress to combat this risk.

However, this awareness has not yet translated into support for the CISO. This research has shown that the C-Suite still expect the CISO to work long hours, want them to deliver even more value, and ultimately hold them responsible for a security breach if it does occur. These expectations and beliefs need to be challenged if the CISO's working life is to improve.

The next step is for the board to take action to help the CISO in their role, which will result in better outcomes for the business. Strong communication channels between the CISO and the board are crucial in achieving this – as it will allow the CISO to voice both their challenges and where they are adding value to the business.

Improving the relationship between the CISO and the board – and in the process improving the CISO's working life – can only have positive outcomes from the business. With a strong and empowered CISO at the head of their security team, organizations will face less risk, be better protected, be more able to deal with a security breach when it hits, and ultimately become safer from cyber crime.

ABOUT NOMINET

Nominet is driven by a commitment to use technology to improve connectivity, security and inclusivity online. For over 20 years, Nominet has run the .UK internet infrastructure, developing an expertise in the Domain Name System (DNS) that now underpins sophisticated network detection and response that is used in by governments and enterprises to mitigate cyber threats.

A profit with a purpose company, Nominet supports initiatives that contribute to a vibrant digital future and has donated over £47 million to tech for good causes since 2008, benefitting more than 10 million people. The company has offices in Oxford and London in the UK and Washington D.C in the US.

Nominet delivers the Protective DNS (PDNS) service on behalf of the UK's National Cyber Security Centre (NCSC). Part of the UK Government's Active Cyber Defence program since its inception in 2016, the PDNS service improves the cyber resilience of the UK. Nominet is also working with other governments around the world to deliver similar PDNS services.

Nominet's network detection and response platform, NTX, is founded on the expertise and experience gained while protecting part of the UK's critical national infrastructure. It offers network detection and response to organizations across the world, including Haas F1, GWR and RS Components.

NOMINET NTX

NTX is purpose-built to analyze billions of DNS data packets in real time, pinpointing and eradicating malicious activity quickly and effortlessly.

NOMINET NTXPROTECT

NTXprotect is Nominet's complete threat monitoring, blocking and analytics platform, run by your in-house security team, with optional help from our experts. The platform is compatible with the DNS service your organization is using.

NOMINET NTXSECURE

NTXsecure offers all the benefits of NTXprotect - full threat detection, analytics and proactive blocking – along with a fully-managed, secure DNS service. All this is run for you by our exceptional team of DNS experts and security analysts.

NOMINET

For more information on how Nominet can help secure your organization, please contact us on:
UK: +44 (0)1865 332 255 | USA: +1 202 821 4256 | info@nominetcyber.com | nominetcyber.com