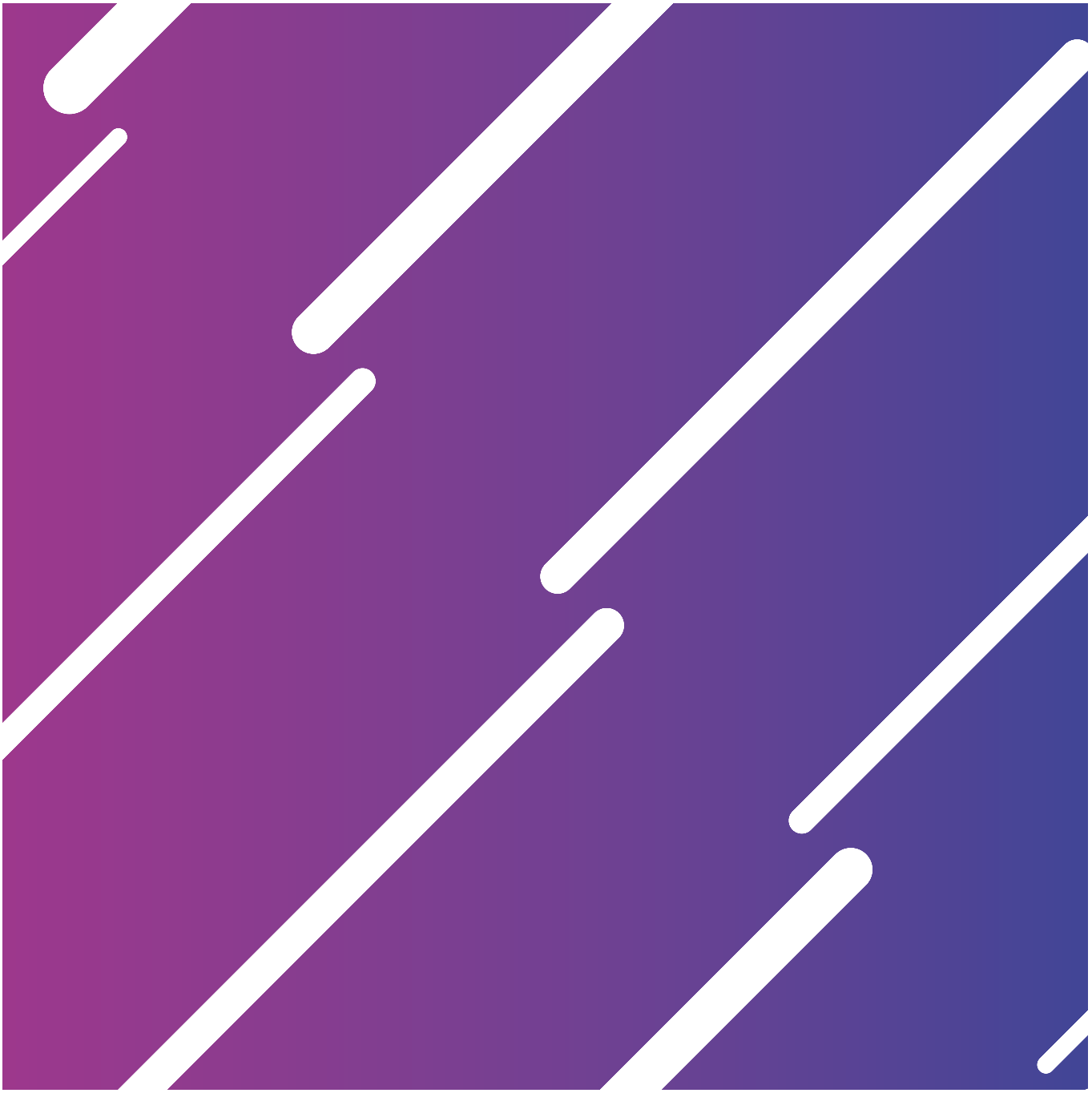


LIFE INSIDE THE PERIMETER

Understanding the modern CISO

NOMINET CYBER SECURITY

EXTERNAL THREATS, INTERNAL PRESSURES

Foreword:
Russell Haworth
CEO, Nominet

In a sector dominated by vast datasets and hinging its future on increased automation, it might appear counterintuitive to carry out a piece of research focussing on people. Being the pragmatic sector it is, our focus tends to be on technical solutions to technical problems. However, step back and technology is just the plain on which the battle manifests. At the start and end of every attack, there are people; whether this is a criminal launching attacks or a security team trying to stop them. Understanding them is therefore crucial.

That is what this research is all about. Despite the job title, the modern CISO's role has always been predominantly people-focussed. Acting as a decision maker trapped between highly technical IT staff and business-focussed leadership teams requires a unique skill-set. The modern CISO is just as much diplomat and translator as they are technologist and IT security person. How well they navigate this split personality to build advocacy with the board, whilst also delivering what operational teams want, often dictates the effectiveness of their defence.

Our work with senior security leaders also teaches us that this is becoming enmeshed with an emerging and yet very human issue, that of being increasingly overwhelmed. This is being driven by a number of factors including increased threat volumes and the continual elevation of cyber security as a business issue.

Given our background supporting the security community, we thought this an interesting and unexplored issue to delve into. It was not all altruism, as many of the findings will be used to support the go-to-market approach of our new cyber security solution that is operating at the DNS level, NTX. Also, as anyone in the space knows, there is a lot of hyperbole associated with cyber security products - so this is our attempt to get under the skin of the human element.

NOMINET
NTX PLATFORM

METHODOLOGY AND EXECUTIVE ANALYSIS

Nominet commissioned Osterman Research to conduct a survey of 408 CISOs overseeing security for organisations with a mean average of 8,942 employees. This comprises 207 companies in the USA and 201 companies in the UK, spread across a range of sectors. The objective was to collect and analyse a large enough dataset to make valid conclusions into the opinions, behaviours and mindset of those making cyber security decisions at large organisations.

The findings paint an interesting human picture often forgotten against a backdrop of technical threat analysis. The data shows a narrative comprising of three distinct parts:

Nearly 70% discovered malware hidden on their networks for an unknown period of time

Less than a third are in their job for more than three years

Nearly 17% of CISOs are either medicating or using alcohol to deal with job stress

1 BALANCING RESOURCES WITH THE INEVITABILITY OF BREACH

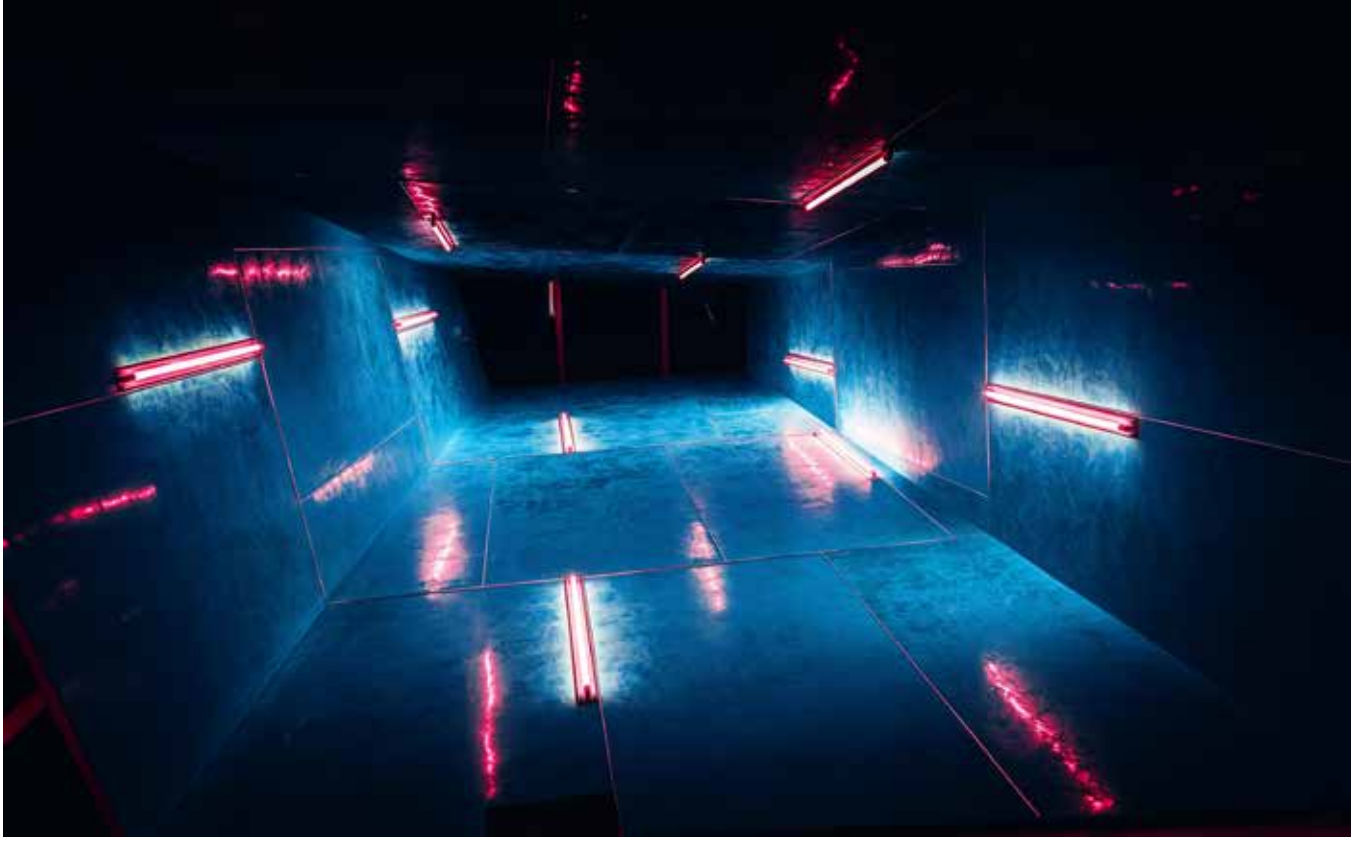
The majority of CISOs say they don't have enough resources to defend the organisation they are trying to protect, with the largest deficit being people. This reduces security effectiveness, with nearly 70% having found malware hidden on their networks for an unknown period of time – in some cases over a year.

2 BOARDS STILL DON'T UNDERSTAND, CREATING JOB INSECURITY

A fraction of board members have an in-depth understanding of cyber and whilst CISOs feel their role is seen as valuable, it is still not widely accepted as a strategic function. Despite the fact 60% feel the board understands the inevitability of a breach, a third still expect to be fired or disciplined if the worst happens. Less than a third are in their job for more than three years.

3 CISOs FIND IT HARD TO DISCONNECT AND ARE EXPERIENCING DAMAGING STRESS LEVELS

Every single CISO questioned found their role stressful, with 91% saying they suffer moderate or high stress and 60% adding they rarely disconnect. 88% of CISOs surveyed are also doing more than the average 40 working hour weeks. Worryingly, a quarter think the job has had an impact on their mental or physical health, with the same stating that it has had an impact on their personal and family relationships. Nearly 17% of CISOs are either medicating or using alcohol to deal with job stress.



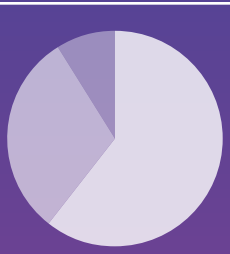
BALANCING THE INEVITABILITY OF BREACH WITH RESOURCES

One of the most common opinions which has emerged in the security space over the last few years is the acceptance of inevitability of cyber breach. With every aspect of business now digital, the attack surface has grown accordingly and gone are the days when security teams could hope to easily keep the entire enterprise watertight. Anywhere a line of code is present now provides an opportunity for attack, regardless of sector.

Seemingly inevitable, yet unseen

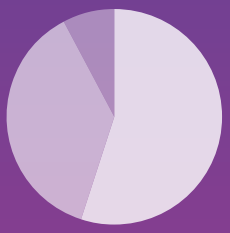
Against this backdrop, over 60% of CISOs questioned admitted to having found malware which had been hidden in their infrastructure for an unknown period of time. Perhaps just as worryingly, another 9% of those questioned said they simply 'weren't sure' when asked if this had happened. Only a third claimed to have full visibility of threats in their organisation, or had remained malware free.

HAS YOUR SECURITY TEAM EVER DISCOVERED MALWARE THAT HAS BEEN HIDDEN IN THE INFRASTRUCTURE FOR AN UNKNOWN PERIOD OF TIME?



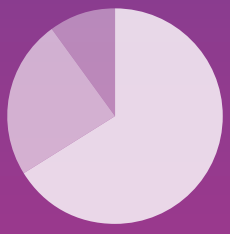
OVERALL

YES	60.5%
NO	30.6%
NOT SURE	8.8%



USA

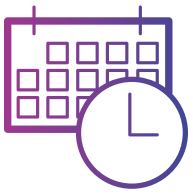
YES	55.1%
NO	37.2%
NOT SURE	7.7%



UK

YES	66.2%
NO	23.9%
NOT SURE	10.0%

Of those that admitted being affected by a security incident, the average length of time before discovering it had occurred was 14 days. Interrogating the data in more detail reveals that over 40 of those who responded didn't find anything for three months, many extending as far as six months and one anonymous CISO admitted to a period of 400 days lapsing before they were able to uncover the threat. When comparing response times across the Atlantic, British CISOs lag behind their American counterparts somewhat – taking almost twice as long to respond at an average of 18 days, compared with 9.5.



One anonymous CISO admitted to a period of 400 days lapsing before they were able to uncover the threat

WHAT IS THE AVERAGE LENGTH OF TIME, IN DAYS, THAT IT TAKES FOR A SECURITY INCIDENT TO BE DISCOVERED, AND WHAT HAS BEEN THE LONGEST AND SHORTEST TIMES FOR SUCH AN INCIDENT TO BE DISCOVERED?

We realised this might be a difficult question to answer, so your best estimate will be appreciated.

AVERAGE DAYS TO DISCOVER A SECURITY INCIDENT

OVERALL	USA	UK
13.7	9.7	17.9

LONGEST NUMBER OF DAYS IT HAS TAKEN

OVERALL	USA	UK
42.4	38.2	46.7

SHORTEST NUMBER OF DAYS IT HAS TAKEN

OVERALL	USA	UK
5.4	3.2	7.6

Despite the apparently flawed nature of defences overall, the data showed that CISOs agreed that a lack of resources hold back an effective security posture. More than half of those questioned (57%) said they were suffering from inadequate budgets, and 63% said they were struggling to put in place the right people. Interestingly however, the leading organisational factor cited as a problem was a lack of senior management buy-in to the advice of security employees, with over 65% saying this was an issue.

ON A SCALE OF 1 TO 7, HOW ADEQUATE ARE THE FOLLOWING IN YOUR ORGANISATION IN DEFENDING AGAINST A SEVERE CYBERATTACK, WHERE 1 IS "NOT ADEQUATE AT ALL" AND 7 IS "VERY ADEQUATE"?

BUDGET

OVERALL	USA	UK
43.4%	39.6%	47.3%

ADVANCED TECHNOLOGY

OVERALL	USA	UK
50.9%	45.1%	57.6%

PEOPLE RESOURCES

OVERALL	USA	UK
36.6%	33.5%	39.8%

SENIOR MANAGEMENT ACCEPTANCE AND BUY-IN OF ADVICE OF SECURITY EMPLOYEES

OVERALL	USA	UK
35.9%	36.9%	34.8%

Figures indicate responses of 6 or 7.

DOES A SENIOR JOB IN SECURITY LEAD TO JOB INSECURITY?

Across the board, there was an overarching feeling amongst the CISOs questioned that, whilst their work is appreciated by senior management teams, it is still yet to be seen as strategically valuable. The data suggests that this is perhaps due to a lower than ideal level of understanding of the realities and details amongst the board. However intangible this problem sounds, it is unfortunately manifesting in a very real manner with many CISOs feeling that, if the inevitable beach does happen, their job would be at risk.

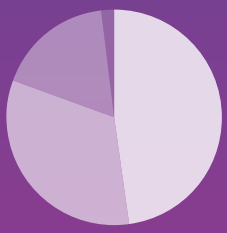
The majority of CISOs polled agree that at least one member of the executive management team should be a security expert. However, this is at odds with the reality. Despite 70% agreeing a cyber security specialist should be on the board, fewer than 6% say they have a member who is highly knowledgeable of the issue. 30% of those questioned even said the executive team had no expertise at all.

70% agree a cyber security specialist should be on the board

OVERALL, HOW MUCH EXPERTISE WOULD YOU SAY YOUR BOARD MEMBERS AND EXECUTIVE MANAGEMENT HAVE WITH REGARD TO TRULY UNDERSTANDING THE NUANCES AND IMPLICATIONS OF CYBER SECURITY ISSUES?

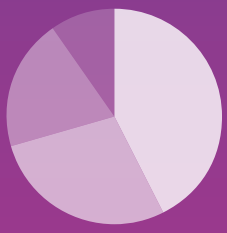
OVERALL

NONE	30.4%
SOME	45.3%
QUITE A BIT	18.6%
A GREAT DEAL	5.6%



USA

NONE	32.9%
SOME	47.8%
QUITE A BIT	17.4%
A GREAT DEAL	1.9%



UK

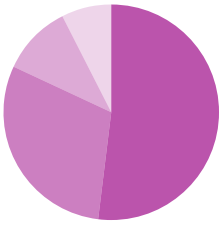
NONE	27.9%
SOME	42.8%
QUITE A BIT	19.9%
A GREAT DEAL	9.5%

"The lack of cybersecurity expertise on boards underscores the disconnect between CISOs and the rest of the organizational leadership team. It is difficult to expect the proper level of governance and oversight with such an inherent absence of understanding of the risk at that level. Because almost all organizations and attackers rely on DNS, a strategy of monitoring this traffic to identify and stop threats is an essential but often overlooked component of an effective network security approach."

Bradley Schaufenbuel
Chief Information Security Officer and VP at Paylocity

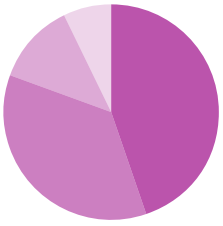
CISO perceptions of the underlying opinions of the board on security perhaps throws some light onto why this is. Given the broader focus of senior business leaders to drive revenues and protect brand, cyber security is still not widely accepted as a strategic function. Only around half (52%) of CISOs felt executive teams valued the security team from a revenue and brand protection standpoint; this was distinctly lower in the USA (44%) than the UK (60%). Unfortunately, 18% of those questioned even thought their board was indifferent to the security team, or saw them as an inconvenience.

HOW DO YOU THINK THE EXECUTIVE MANAGEMENT (BUSINESS/NON-TECHNICAL) AND BOARD OF DIRECTORS AT YOUR ORGANISATION VIEW THE SECURITY TEAM?



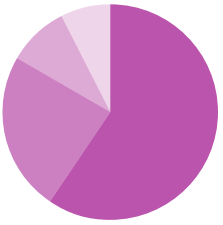
OVERALL

IMPORTANT	52.2%
GOOD TO HAVE	29.9%
NEUTRAL	10.5%
NEGATIVE	7.4%



USA

IMPORTANT	44.9%
GOOD TO HAVE	35.7%
NEUTRAL	12.1%
NEGATIVE	7.2%

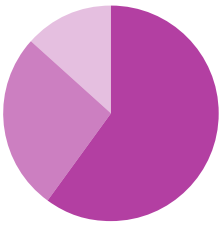


UK

IMPORTANT	59.7%
GOOD TO HAVE	23.9%
NEUTRAL	9.0%
NEGATIVE	7.5%

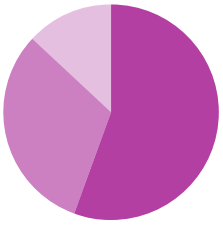
Crucially in setting the environment in which the CISO works, this lack of education means that only 60% of CISOs think their CEO / President agrees a breach is inevitable. Couple this with the fact that nearly a third (32%) of all those questioned believe that, in the event of a breach they would either lose their job or receive an official warning, and it adds significant individual pressure. Interestingly, a greater percentage of UK CISOs think they would receive a warning or be fired (37%) in the event of a breach, against just 28% in the US.

DO YOU BELIEVE THE EXECUTIVE MANAGEMENT TEAM (PRESIDENT/CEO-LEVEL) IN YOUR ORGANISATION UNDERSTANDS AND ACCEPTS THAT SECURITY BREACHES ARE INEVITABLE?



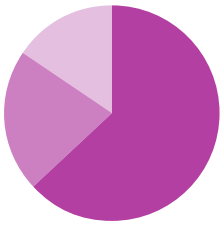
OVERALL

YES	60.0%
NO	26.7%
NOT SURE	13.2%



USA

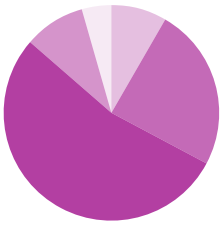
YES	57.0%
NO	31.9%
NOT SURE	11.1%



UK

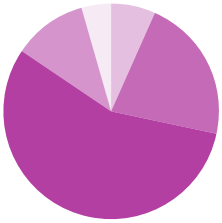
YES	63.2%
NO	21.4%
NOT SURE	15.4%

IF THERE WAS A SIGNIFICANT SECURITY BREACH IN YOUR ORGANISATION, HOW DO YOU BELIEVE THAT EXECUTIVE MANAGEMENT IN YOUR ORGANISATION WOULD RESPOND?



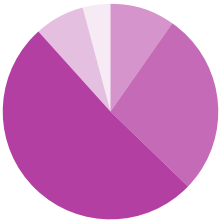
OVERALL

TERMINATED	8.6%
OFFICIAL WARNING	24.5%
ASSIST IN RESOLVING	53.7%
UNCONCERNED	9.3%
NOT SURE	4.2%



USA

TERMINATED	6.8%
OFFICIAL WARNING	21.7%
ASSIST IN RESOLVING	56.0%
UNCONCERNED	11.1%
NOT SURE	4.3%

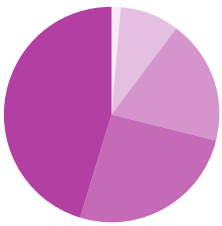


UK

TERMINATED	10.0%
OFFICIAL WARNING	27.4%
ASSIST IN RESOLVING	51.2%
UNCONCERNED	7.5%
NOT SURE	4.0%

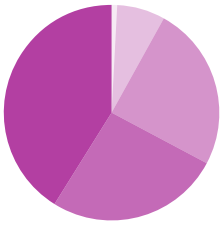
It is arguable this is helping to create an environment of higher job churn for CISOs when compared with the average worker. In total, the majority of CISOs said average job length was less than three years (55%) with nearly a third (30%) saying less than two years. This is at odds with available data on average job tenure; which the US Dept. of Labour sets at 4.2 years. US senior security staff tend to churn slower than those in the UK, with 67% being in their job over two years compared to the UK (75%).

IN YOUR EXPERIENCE, WHAT IS THE AVERAGE TENURE OF SOMEONE IN A SENIOR SECURITY ROLE?



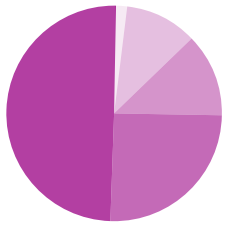
OVERALL

UP TO 6 MONTHS	0.2%
6 – 12 MONTHS	1.2%
12 – 18 MONTHS	9.1%
18 MONTHS – 2 YEARS	18.6%
2 – 3 YEARS	25.7%
3 YEARS +	45.1%



USA

UP TO 6 MONTHS	0.0%
6 – 12 MONTHS	1.0%
12 – 18 MONTHS	7.2%
18 MONTHS – 2 YEARS	24.6%
2 – 3 YEARS	26.1%
3 YEARS +	41.1%



UK

UP TO 6 MONTHS	0.5%
6 – 12 MONTHS	1.5%
12 – 18 MONTHS	10.9%
18 MONTHS – 2 YEARS	12.4%
2 – 3 YEARS	25.4%
3 YEARS +	49.3%

INSIDER INSIGHT

An anonymous senior security figure in a major corporation with a market cap of $1bn+ reflecting on their experience of a number of incidents and data breaches, said:

"When it happened, the management team very quickly escalated the situation beyond members of the technical security team, even though they had valuable specialist knowledge. Their presence was not required in the room where decisions were made. Once the media became involved, corporate politick drove the situation. It made effective response harder and ultimately, I believe best-practice suffered.

"In general, boards like to talk about being security friendly, but I don't believe that is the case. It seems more for show. In my experience, I found that security initiatives played second fiddle to protecting a margin somewhere. We were handling vast amounts of very valuable data, but the squeeze on resources seemed to come first.

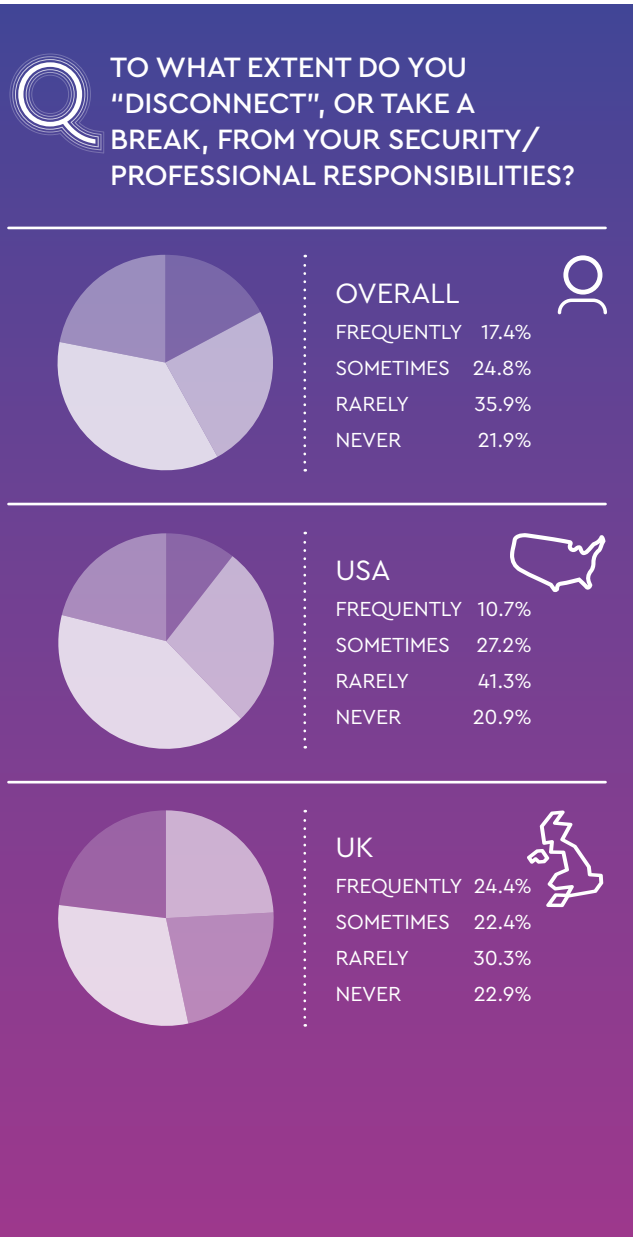
"It's a very stressful industry, no doubt. You are often faced with an impossible position, trapped between internal teams, auditors, compliance teams, regulators and numerous extremely challenging technical situations, for which there are no quick, easy and cheap fixes. The pace of technological change combined with the desire to exploit the latest and greatest solutions just adds to the overall complexity and pressure. For frontline teams, the people monitoring threats are okay because they just pass it on up the ladder. However, when you have to report and action threats to exec teams, that's when the stress starts to build because you are delivering unwelcome news which is often also seen as a failing.

"I definitely used to take it home, in times of stress I would try to cope by escaping to the countryside with my partner trying to seek some "time out". However even then, I found that we would be walking along together and suddenly, to my surprise, my partner would say to me: "Will you please stop talking about work! We're trying to relax here!" It was really hard to truly switch off. I would suffer physically too, illness would take longer to shake off for example."

THE HUMAN COST OF A DIGITAL PROBLEM

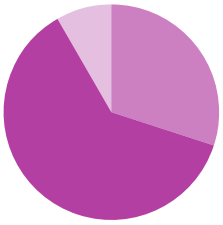
This confluence of factors is putting many CISOs in an isolated and stressful position. To summarise, threats are still infiltrating large organisations for periods long enough to cause significant damage, however resources for countermeasures are not always sufficient. To compound the issue, boards seemingly don't have the required understanding or desire for security to become a strategic function. This is potentially creating fertile ground for breaches, for which ultimately the CISO may be held responsible.

In response, CISOs are working hard. Nearly 60% of those questioned either 'rarely or never' disconnect from their security duties, with 22% saying they are available virtually 24/7. The US CISO is particularly bad at getting downtime, with 89% saying they never have a break for two weeks or more. This is also represented in the number of hours the CISO is working, with 88% saying they work more than a 40 hour week; 54% between 41 and 50 hours, 27% at between 50 and 60 hours and 7% at 85 hours per week. One respondent was working 100 hour weeks. Compare this with official data on the average hours worked by full time employees in the US (40.85 hours) and UK (37.3 hours) and it is significantly more.



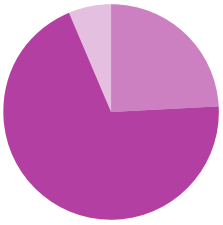
This situation is contributing to a not insignificant feeling of anxiety for the CISO. In fact, 100% of those questioned said the security team's job was stressful. Questioned on a sliding scale, 91% of CISOs put the average security employee's job at a level of 'moderate or high stress' – with over a third (36%) of UK teams feeling 'tremendous' stress levels. When asked which technical facet of the job drove the most stress, CISOs mostly commonly pointed the finger at 'staying ahead of threats' (33%), followed by securing the network (28%) and securing endpoints (26%). Crucially in setting the environment in which the CISO works, this lack of education means that only 60% of CISOs think their CEO / President agrees a breach is inevitable. Couple this with the fact that nearly a third (32%) of all those questioned believe that, in the event of a breach they would either lose their job or receive an official warning, and it adds significant individual pressure. Interestingly, a greater percentage of UK CISOs think they would receive a warning or be fired (37%) in the event of a breach, against just 28% in the US.

WHAT IS THE STRESS LEVEL FOR THE AVERAGE EMPLOYEE ON YOUR ORGANISATION'S SECURITY TEAM?



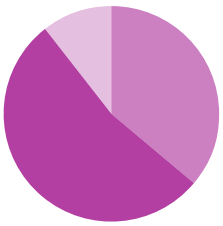
OVERALL

TREMENDOUS	30.1%
MODERATE	61.5%
LOW	8.3%
NONE	0.0%



USA

TREMENDOUS	24.2%
MODERATE	69.6%
LOW	6.3%
NONE	0.0%



UK

TREMENDOUS	36.3%
MODERATE	53.2%
LOW	10.4%
NONE	0.0%

For the CISO, the personal cost seems to be accumulating. Over a quarter of those questioned (26.5%) said the stress of the job is impacting their physical or mental health. Just as worryingly, nearly a quarter (23%) admitted that the job had also eroded personal relationships. As more of a professional concern, 27.5% of CISOs also admit that stress levels are affecting their ability to do their job.

ON A SCALE OF 1 TO 7, TO WHAT EXTENT HAS STRESS IN YOUR JOB AFFECTED THE FOLLOWING, WHERE 1 IS "NOT AT ALL" AND 7 IS "A GREAT DEAL"?

RELATIONSHIPS AT WORK

OVERALL	USA	UK
27.0%	27.1%	26.9%

RELATIONSHIPS OUTSIDE OF WORK

OVERALL	USA	UK
23.3%	21.8%	24.9%

YOUR PHYSICAL OR MENTAL HEALTH

OVERALL	USA	UK
26.5%	25.7%	27.4%

YOUR ABILITY TO DO YOUR JOB

OVERALL	USA	UK
27.3%	21.8%	32.8%

Figures indicate responses of 6 or 7.

ON A SCALE OF 1 TO 7, HOW DO YOU DEAL WITH THE STRESS OF YOUR JOB BY PARTAKING IN EACH OF THE FOLLOWING, WHERE 1 IS "NEVER" AND 7 IS "VERY FREQUENTLY"?

EXERCISE

OVERALL	USA	UK
25.1%	27.2%	22.9%

TAKING FREQUENT BREAKS DURING THE WORK DAY

OVERALL	USA	UK
20.4%	17.1%	23.9%

MEDICATION

OVERALL	USA	UK
7.1%	6.8%	7.5%

THINKING ABOUT WHEN "HAPPY HOUR" STARTS AT MY FAVORITE PUB/BAR/RESTAURANT

OVERALL	USA	UK
9.4%	4.4%	14.4%

MEDITATION OR PRAYER

OVERALL	USA	UK
12.1%	10.2%	13.9%

READING, PODCASTS/RADIO, VIDEOS/TV

OVERALL	USA	UK
27.1%	31.2%	22.9%

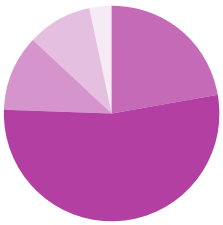
DAYDREAMING ABOUT THE NEXT VACATION

OVERALL	USA	UK
13.8%	10.7%	16.9%

Figures indicate responses of 6 or 7.

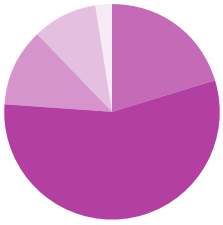
From a technological perspective, in terms of the automated AI driven approach being taken by many cyber security vendors to address some of the burden on humans, it seems the CISO is broadly positive with three-quarters (75%) agreeing it will have a positive impact.

WHAT IMPACT DO YOU ANTICIPATE THAT AUTOMATION AND AI WILL HAVE ON MAKING YOUR SECURITY ROLE LESS STRESSFUL?



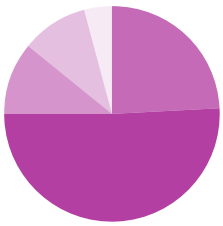
OVERALL

DRAMATICALLY	22.4%
SOMEWHAT	53.3%
NO IMPACT	11.3%
MORE STRESSFUL	9.8%
NOT SURE	3.2%



USA

DRAMATICALLY	20.4%
SOMEWHAT	55.8%
NO IMPACT	11.7%
MORE STRESSFUL	9.7%
NOT SURE	2.4%



UK

DRAMATICALLY	24.4%
SOMEWHAT	50.7%
NO IMPACT	10.9%
MORE STRESSFUL	10.0%
NOT SURE	4.0%

EXPERT OPINION

Dr Dimitrios Tsivrikos, a business psychologist and lecturer at University College London, provides his insight into the report findings:

CISOs are a group of employees faced with the overwhelming pressure of adopting, protecting and safeguarding private and business data. As these employees are tasked with dealing with two incredibly challenging sectors – tech and security – they often struggle to communicate the importance of their work without raising alarms to their management, who might worry about the potential brand, financial and security threat that could result from a data compromise. This can leave CISOs in an emotional limbo, as no one fully understands the complexity, skill and importance of their work, and contemporary management often neglects to invite them to join the decision-making boards within a given business. Such emotional instability poses a clear threat to an employee's well-being, a fact that has ramifications for a CISO's productivity, vigilance and overall performance.

Both academic and field data provides clear support that employees who experience high levels of stress are twice as likely to take sick leave, underperform and miss opportunities for promotion. In addition, individuals who are stressed at work are oftentimes not living their best lives privately, either. Most of us find it difficult to suppress the pressures from work, and they do indeed spill over into our private life. This poses significant health-related threats to personal well-being as individuals rely on alcohol and other non-constructive behaviours in order to relax and find relief from those pressures.

So from an organisational perspective, it is of paramount importance that we address organisational stress among employees in all work sectors. And extra emphasis ought to be paid to CISOs, as errors in their judgment, caused by excessive work-related stress, can indeed have detrimental effects upon business and personal data. We often recommend to business and individuals to follow the following steps:

1. Be proactive and informed about the right tools that are available to protect your business from a potential cyber attack

2. Be vocal about your levels of stress to both work colleagues as well as family. You will be surprised by the supportand help that is often available via both official and unofficial channels. Silence kills when it comes to stress-related incidents.

3. Explore healthy ways of decompressing at home. Trust me – alcohol and excessive eating are short-term solutions, and won't provide the long-term benefits that will relax you and energise you for a busy work day. Increasing your level of exercise can be a great way to unwind and build confidence in dealing with day-to-day stressful situations.

IN SUMMARY

Russell Haworth, CEO, Nominet

For me, this piece of research has proven some existing assumptions about the environment in which today's security leaders work, and shone a light on some unexpected problem areas. These are all rooted in three macro industry trends, namely a larger attack surface, the fast pace of innovation from a well-resourced adversary and growing volumes of cyber threats. Ultimately, for the CISO this means more attacks at a faster pace and an increased chance of breach.

The data collected marks CISOs as a strongly motivated set of individuals, keen to address this challenge. To help this happen to its fullest, organisations need to consider a number of tactical and strategic factors.

Most importantly, a cultural change needs to occur at board level. To really empower security leaders, cyber security must be reclassified as a strategic, business-critical function and have a solid seat at the table instead of the current lip service many appear to be paying it. Put in management terms, technological change is embraced for the revenue and cost saving benefits it brings, however, if left insecure this asset can very quickly become a liability of negative value. One steals from the other. Such a shift in perception will only come from if management teams invest time understanding the detail or bring specific knowledge onto the board. It is important this is not done against the backdrop of a major incident, so it must be a proactive decision. Responsibility for ensuring this happens lies with both sides of the equation, CISO and management team alike must have open dialogue.

This will, in turn, foster transparency and understanding. A CISO who is doing their role under the sword of Damocles, afraid of losing their job when the inevitable happens, is stressed and ultimately, less effective. However, in a collaborative environment where the risks are well understood, not only will they have confidence to do their job effectively, but they will have a greater chance of receiving the resources required to perform.

Typically, these resources manifest as technology investment or extra headcount, which reduces work and therefore stress levels. However, investing in the personal wellbeing of CISOs should not be overlooked, something which unfortunately seems all too common. Progressive organisations should ensure HR teams recognise this and are able to provide sufficient resource to address the strains of operating on the front line of the modern threat environment.

Finally, whatever a CISO believes on AI and automation, done correctly it has a role to play in reducing stress by making workloads more tolerable. With increasing threat datasets, human monitoring will only ever either become overloaded, or cross a cost / benefit line. Neither is sustainable. Successfully using automation lies in the details, from being selective in the choice of vendors to ensuring any new deployment is 'trained' correctly before being put live. CISOs who are given the time and budget to do so, will reap the personal benefits from decreased stress and, as we have seen, security posture will improve as a result.

ABOUT NOMINET

Nominet is driven by a commitment to use technology to improve connectivity, security and inclusivity online. For 20 years, Nominet has run the .UK internet infrastructure, developing an expertise in the Domain Name System (DNS) that now underpins sophisticated threat monitoring, detection, prevention, and analytics that is used 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 £45 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 U.S.

nominet.uk

NOMINET CYBER SECURITY SERVICES

Nominet's cyber security solution – NTX – cuts through the sea of data teams are working with and gives immediate visibility of threats and anomalies to preserve the integrity of a network.

All networks rely on DNS traffic. But it is often over-looked in the security stack and therefore the 'open back-door' for cyber criminals.

Using patented machine learning techniques, NTX analyses vast volumes of DNS traffic to predict threats, identify infected devices and pinpoint malicious behaviour alerting security teams so action can be taken before these threats become a problem.

Protect your users the way that best suits your business

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 organisation 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.

NTX is being used by the UK's National Cyber Security Centre as part of its Active Defence programme to great effect, stopping 5000 malicious traffic requests every week, countering malware, phishing and data exfiltration attacks.

The technology is a result of Nominet's expertise running the .UK internet infrastructure over the last 22 years. Early versions of the technology helped identify security vulnerabilities and helped the internet community and law enforcement tackle significant botnets.

More details on NTX platform can be found at **nominet.uk/ntx.**

NOMINET

NOMINET
CYBER
SECURITY

For more information on how Nominet can help secure your business, please contacts us on:
UK: +44 (0)1865 332 255 | USA: +1 202 821 4256 | cybersecurity@nominet.uk