



Trouble at the top:

The boardroom battle for cyber supremacy





Real-time DNS-based
threat prediction,
detection and blocking

Contents

Foreword	4
Methodology	5
Executive summary: A state of the nation	5
The findings	6
The missing links: Responsibility	10
The missing links: Budget	15
The missing links: People resources	18
In summary	20
Nomet Cyber Solutions	21
Protect your users the way that best suits your business	21
About Nomet	21

Foreword

In the current landscape of pervasive cyber threats, every business needs a clear strategy that outlines how to deal with and mitigate the risk of attack, as well as a response prepared should the worst happen. However, the lines are often blurred. At the top of every large organisation is a group of very knowledgeable, strong leaders, each with their own skillsets and opinions.

This is where the trouble can start. The structure of boards has remained fairly stagnant, with each member often looking after a certain part of the business. The issue is that criminals are indiscriminate. They don't necessarily target one single business unit, instead attempting to gain access wherever they can. This means that each member of the board may try to "own" cyber security for their particular area. But are they best equipped to do so? Should they instead be deferring to a CISO or security team? Do they have the knowledge to put their own head above the parapet? Are they relying on clever technology to keep them safe?

These are the questions this research attempts to answer.

Sitting at the heart of the UK's digital economy, we work with a number of senior business and government leaders; many of whom have been in their industry for decades. This puts them in the best position to lead their business, but given the ever-changing nature of the cyber landscape, they may not have the right tools to combat this particular threat.

It's in a CEO's nature to want to take responsibility for every part of their business. One of the best lessons I learnt was that you can't be an expert in everything. To that end, I surround myself with industry leading experts who help me run the strongest, most secure business possible. This is especially true when it comes to cyber.

At Nominet, we have a talented team of cyber specialists, all of whom work tirelessly to keep the .UK namespace, and a growing number of government and private businesses, safe from threats.

Without them, my tenure, and more importantly the safety of Nominet, would be in question. I hope that this research demonstrates to some of my fellow business leaders that sometimes it's not about what you know, but who you know.

– Russell Haworth, CEO, Nominet



Methodology

The data this research paper references is based on Vanson Bourne research, which took the input of 400 C-level executives with a mean average of 8,936 employees. This comprises 200 companies in the USA and 200 in the UK, spread across a range of sectors.

Additional data comes from Osterman research which took the input 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.

Do you believe that security breaches are inevitable at your organisation?

	Total	US	UK
Yes	76%	80%	72%
No	19.5%	16%	23%
Don't know	4.5%	4%	5%
Base	400	200	200

Executive summary: A state of the nation

One thing that has remained clear with every piece of research is that cyber attacks are an inevitable part of running a business. Criminals are smart, fast-moving and indiscriminate, and enterprises are struggling to keep up. An acceptance of the inevitable is growing at a board level. Indeed, more than three quarters (76%) of enterprise C-level executives believe that cyber security breaches are now inevitable. Those working in the utilities sector are particularly worried, with almost half (48%) claiming that the risk is "very high".



The findings

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

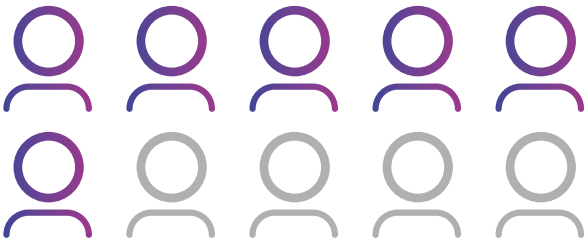
	Total	Financial Services and FinTech	Life sciences and Pharmaceutical	Healthcare	Legal	Utilities	Transport and Logistics	Retail	Automotive	Other public and private sectors
Very high	33.3%	32.5%	17.7%	37.5%	17.1%	48.4%	25%	29.7%	42.1%	39.1%
High	28.8%	37.5%	41.2%	15%	25.7%	29%	40%	37.8%	21.1%	22.9%
Moderate	29%	27.5%	38.2%	32.5%	31.4%	22.6%	27.5%	29.7%	23.7%	28.6%
Low	7.5%	2.5%	2.9%	10%	20%	0%	7.5%	2.7%	13.2%	7.6%
No risk at all	1.5%	0%	0%	5%	5.7%	0%	0%	0%	0%	1.9%
Don't know	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Base	400	40	34	40	35	31	40	37	38	105

Despite the seeming inevitability of attack, nine in ten C-suite members believe that their organisation is lacking at least one resource that would help them to defend against a severe cyber attack, with the most common of these (59%) being advanced technology.



Nine in ten C-suite members believe that their organisation is lacking resources that would help them to defend against a cyber attack

For CEOs and other C-suite members whose priority is keeping customer and client data safe, it's no surprise that the immediate response is to throw technology at the problem.



Six in ten C-suite members believe they lack advanced technology

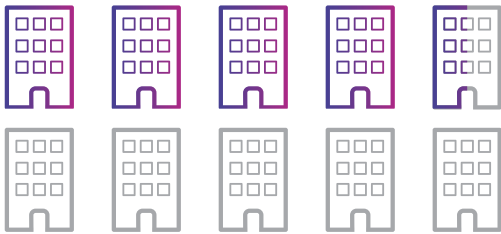


Thinking specifically about how a cyber attack could take control of your systems, which of the following is your organisation most concerned about protecting in the event of such an attack? Combination of responses ranked first, second and third

	Total	US	UK
Customer/client data	64%	64%	64%
Internal organisational data	45%	50%	40%
Operational systems	41.3%	41.5%	41%
Reputation	39.8%	34.5%	45%
Intellectual property	36.8%	36.5%	37%
Revenue	36.5%	38.5%	34.5%
Human life	35%	31.5%	38.5%
Other	0.3%	0.5%	0%
Don't know	0.5%	1%	0%
Base	400	200	200

The truth is much more complex than throwing technology at the problem though. Yes, there are advanced security tools out there that will flag network alerts, quarantine suspicious packets and create aesthetically pleasing reports. But, without the technical expertise to act against these red flags, business leaders are sailing against the wind. Moreover, the problem is compounded further if there isn't budget available for these advanced tools, or the people needed to deploy and maintain them.

Looking deeper at the problem, in more than four in ten organisations, C-level members believe they are lacking senior management acceptance of advice (46%), budget (44%), and people resources (41%). Without these three important ingredients, most cyber security strategies will fail.



More than four in ten organisations, C-level members believe they are lacking senior management acceptance of advice (46%), budget (44%) and people resources (41%)

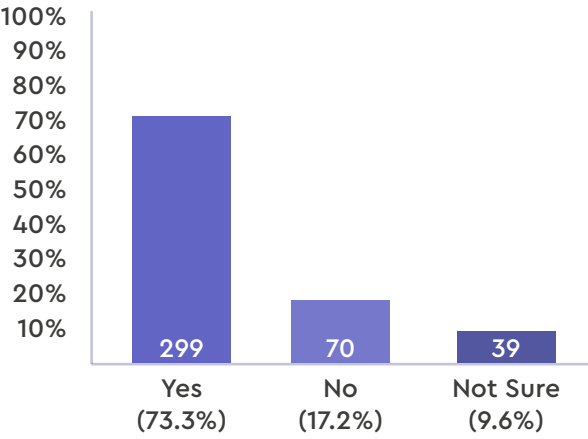
Which of the following resources that are required to defend against a severe cyber-attack do you believe is most lacking in your organisation?

	Total	US	UK
Advanced technology	59%	61%	57%
Senior management acceptance and buy-in of advice by security employees	46%	50.5%	41.5%
Budget	44%	48.5%	39.5%
People resources	41.3%	46.5%	36%
Other	0.8%	1%	0.5%
My organisation is not lacking any resources to defend against a severe cyber attack	9.8%	8.5%	11%
Don't know	0%	0%	0%
Base	400	200	200

Interestingly, CISOs take a different view. In our previous Life Inside the Perimeter: [Understanding the Modern CISO report](#), almost three-quarters (73%) claimed to have the necessary resources to defend against a severe cyber attack.

There's a clear disconnect here. With CISOs and their board counterparts taking markedly different views on the available resources, it's evident that there is some confusion at the top about where the responsibility for cyber security sits, what resources are really available, and how boards, CISOs and security teams can best collaborate to secure their businesses.

Do you believe that your organisation currently has the necessary resources to adequately defend against a severe cyber attack?



The missing links: Responsibility

At board level, more than a third (35%) of respondents believe that the CEO is ultimately in charge of a business' response to a data breach, compared to the CISO (32%). In a way, they are correct: the CEO is at the helm of the business, and their overall concern is for the safety of customer data, and ultimately the continued running of the business. However, there is an expectation that tech alone will keep them safe; it's widely believed that advanced technology is the resource that is most lacking in businesses. But as we've already touched upon, technology is not a panacea. Behind every great software deployment is a CISO – or equivalent figure – who is transcending the gap between technical solutions and business strategy.



Who is ultimately responsible for information security at your organisation?

Chief Executive Officer (CEO)
Chief Information Security Officer (CISO)
Chief Information Officer (CIO)
Chief Technology Officer (CTO)
Other
No single person is ultimately responsible
Don't know
Base

Total	US	UK
34.5%	33%	36%
32.3%	33.5%	31%
19.8%	20.5%	19%
10.8%	10.5%	11%
0%	0%	0%
2.8%	2.5%	3%
0%	0%	0%
400	200	200

In fact, in most cases, it's unlikely that a data breach would be reported to the board. Cyber security incidents are only reported to the board in just 40% of businesses. For the most part, they are flagged to the security team (70%) or the executive/senior management team (61%).

This could be because of an acceptance of an uncomfortable truth: one third of CEOs state that they would terminate the contract of CISOs responsible for not spotting a data breach.



Around two thirds of cases claims that it's unlikely that a data breach would be reported to the board

In your organisation, to whom are cyber security incidents reported?

The security team
The executive/senior management team
The c-suite/board
Other
Incidents are simply recorded or retained "in our system"
Don't know
Base

Total	US	UK
69.5%	74.5%	64.5%
61%	69.5%	52.5%
40%	48%	32%
0.3%	0%	0.5%
1.5%	1.5%	1.5%
0.3%	0%	0.5%
400	200	200

There's also a discrepancy about collaboration at the top in the event of a data breach. Over half (54%) of CISOs believe they would receive help from C-suite members, however, only 38% of the board say they would work with the security team to solve a cyber security issue.

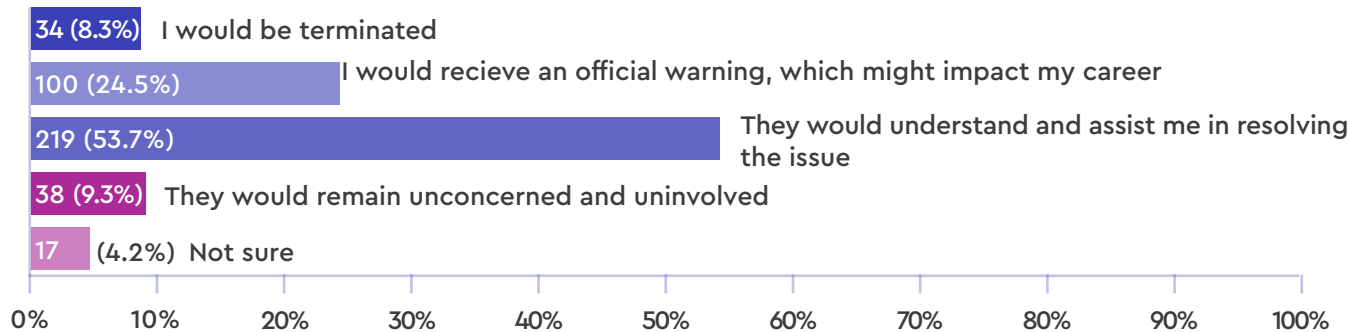


Over half (54%) of CISOs believe they would receive help from other C-suite members

How would your organisation be most likely to respond in the event of a significant security breach?

	Total	US	UK
Understand the issue and assist the security team in resolving it	37.5%	37.5%	37.5%
Termination of the contract/employment of the employee(s) accountable	25.3%	28.5%	22%
Termination of your contract/employment	13.3%	13.5%	13%
Deliver the employee(s) accountable with an official warning	12.8%	10.5%	15%
Refrain from getting involved and let the security team deal with it	10.3%	9.5%	11%
Other	0.5%	0%	1%
Don't know	0.5%	0.5%	0.5%
Base	400	200	200

If there was a significant security breach in your organisation, how do you believe that executive management in your organisation would respond?



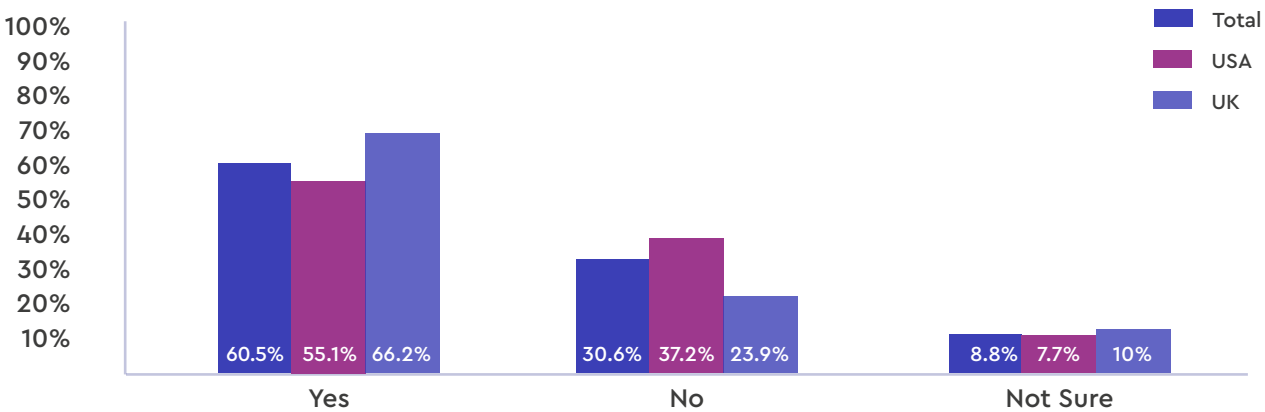
Despite a willingness to collaborate, the majority (71%) of the C-suite concede that they have gaps in their knowledge when it comes some of the main cyber threats facing businesses today; the most common of which being malware (78%). This is alarming, given the fact that 70% of businesses admit to having found malware hidden on their networks for an unknown period of time - in some cases, for over a year.




The majority (71%) of the C-suite concede that they have gaps in their knowledge when it comes some of the main cyber threats




Has your security team ever discovered malware that has been hidden in the infrastructure for an unknown period of time?




Do you think that there are any gaps in your knowledge when it comes to the following types of cyber attacks?




	Total	US	UK
Yes, significant gaps	31.5%	33.5%	29.5%
Yes, some gaps	46.5%	44.5%	48.5%
No, there are no gaps	22%	22%	22%
Base	400	200	200




	Total	US	UK
Yes, significant gaps	24.3%	21.5%	27%
Yes, some gaps	45.8%	47.5%	44%
No, there are no gaps	30%	31%	29%
Base	400	200	200



	Total	US	UK
Yes, significant gaps	22.5%	25.5%	19.5%
Yes, some gaps	45.8%	46%	45.5%
No, there are no gaps	31.8%	28.5%	35%
Base	400	200	200



	Total	US	UK
Yes, significant gaps	24.5%	27%	22%
Yes, some gaps	41.3%	41%	41.5%
No, there are no gaps	34.3%	32%	36.5%
Base	400	200	200



	Total	US	UK
Yes, significant gaps	22.5%	23.5%	21.5%
Yes, some gaps	49.5%	46.5%	52.5%
No, there are no gaps	28%	30%	26%
Base	400	200	200

Despite cyber security being on the board's agenda on a weekly or fortnightly basis (51%), it appears that when push comes to shove, collaboration is lacking in many cases.

With gaps in the knowledge of many C-level respondents, it is surprising that many are still reluctant to collaborate with, or accept advice

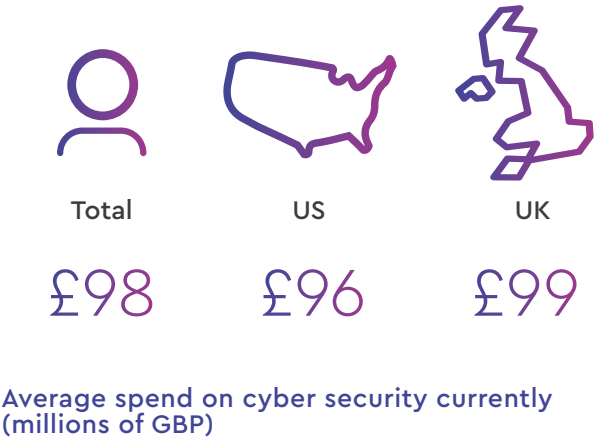
from, the security team when it comes to defending against an attack. It might be time for owners, CEOs, and MDs to hand over control of cyber security decisions to senior members of the security team, which could ultimately see the organisation become much more secure.

What percentage of your organisation's annual IT budget is currently allocated toward cyber security?

	Total	US	UK
0%	0%	0%	0%
1-5%	3%	1%	5%
5-10%	12.8%	10.5%	15%
10-15%	19.5%	16%	23%
15-20%	19%	18.5%	19.5%
20-25%	16.5%	17.5%	15.5%
25-30%	13%	14%	12%
30-40%	8%	11.5%	4.5%
40-50%	7.5%	10.5%	4.5%
More than 50%	0%	0%	0%
Don't know%	0.8%	0.5%	1%
Average (percentage)	20.4%	22.7%	18.1%
Base	400	200	200

The missing links: Budget

On average, 20% of organisations' annual IT budgets are currently being allocated towards cyber security, with this proportion set to rise to 22% over the next 12 months. In real terms, this equates to an average spend of £98m currently, with a forecast increase to £103m with investment only growing in line with inflation despite risks increasing.



This of course changes from sector to sector. The financial services industry, perhaps unsurprisingly, spends much more than other verticals, committing £172m per year on average.



What percentage of your organisation's annual IT budget is currently allocated toward cyber security?

	Total	Financial Services and FinTech	Life Sciences and Pharmaceutical	Healthcare	Legal	Utilities	Transport and Logistics	Retail	Automotive	Other public and private sectors
0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
1-5%	3%	0%	8.8%	7.5%	2.9%	0%	0%	2.7%	2.6%	2.9%
5-10%	12.8%	12.5%	11.8%	20%	17.1%	9.7%	17.5%	5.4%	18.4%	8.6%
10-15%	19.5%	15%	20.6%	15%	14.3%	9.7%	27.5%	32.4%	26.3%	17.1%
15-20%	19%	20%	14.7%	15%	28.6%	32.3%	17.5%	21.6%	7.9%	18.1%
20-25%	16.5%	10%	20.6%	15%	11.4%	22.6%	27.5%	10.8%	13.2%	17.1%
25-30%	13%	12.5%	14.7%	7.5%	14.3%	22.6%	2.5%	0%	23.7%	16.2%
30-40%	8%	22.5%	8.8%	10%	8.6%	3.2%	7.5%	5.4%	2.6%	5.7%
40-50%	7.5%	7.5%	0%	7.5%	0%	0%	0%	18.9%	5.3%	14.3%
More than 50%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Don't know%	0.8%	0%	0%	2.5%	2.9%	0%	0%	2.7%	0%	0%
Average (percentage)	20.4%	23.3%	18.1%	19%	18.2%	20%	17.3%	21.8%	18.9%	22.8%
Base	400	40	34	40	35	31	40	37	38	105
Average spend on cyber security currently (millions of GBP)	£98	£172	£45	£89	£73	£91	£50	£91	£79	£127

Similar to deploying advanced technology, setting aside large cash reserves won't keep a business safe. It's all about how that cash is used. Spending millions on systems that claim to catch all cyber threats but failing to invest in the right people to sit behind that system is a risky strategy.

The missing links: People resources

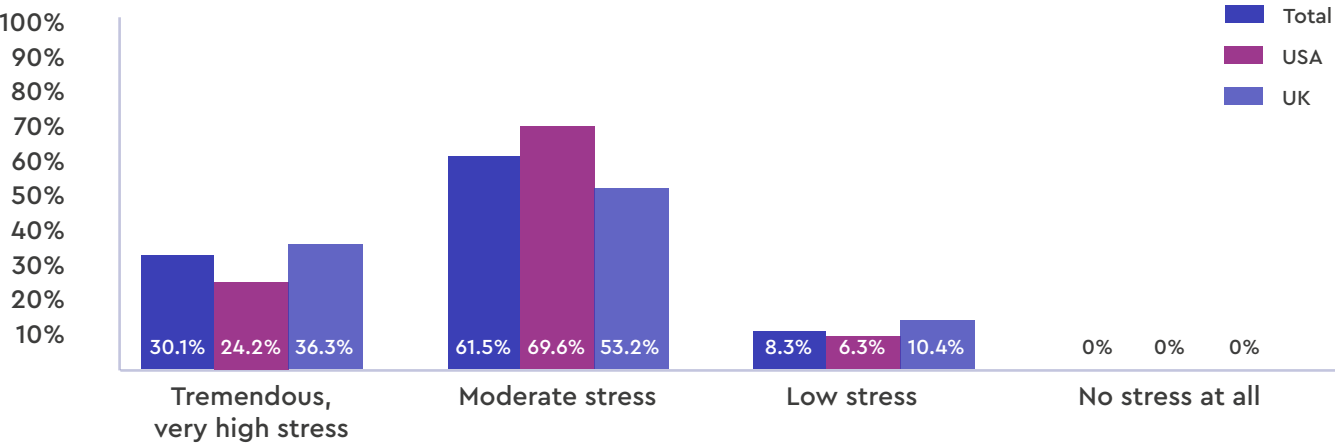
Many enterprises already have an invaluable asset at their disposal: the CISO. However, many are not recognising these important people in the right way, and this is having a damaging effect on the CISO.

Over a quarter of CISOs (27%) said the stress of their job is impacting their physical or mental health. Just as worryingly, nearly a quarter (23%) admitted that the job had also affected their personal relationships. As more of a professional concern, 28% of CISOs also admit that stress levels are having an adverse effect on their ability to do their job.

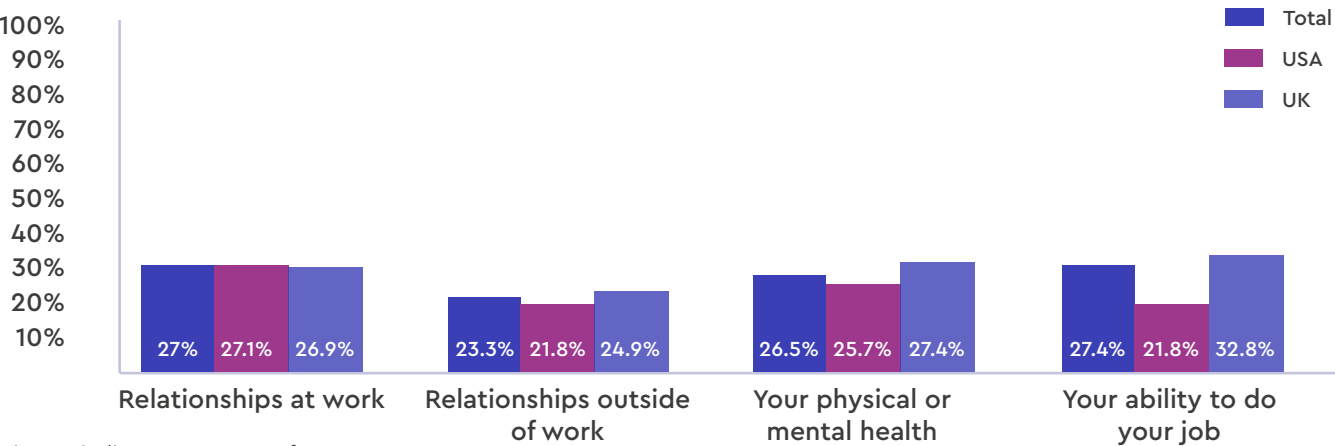
They also feel unsupported: only half of CISOs felt the rest of the executive team valued the security team from a revenue and brand protection standpoint. Worryingly, 18% thought the board was indifferent to the security team, or saw them as an inconvenience.

However, support for CISOs is actually higher than they think. When asked, only 52% of CISOs believe that the board of directors see them as a "must have", but in reality, 76% of C-level executives feel this way.

What is the stress level for the average employee on your organisation's security team?



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"?



Figures indicate responses of 6 or 7

How do you view your organisation's security team?

Necessary: a "must have" business enabler or group that ensures revenue and brand protection	
Good to have: a group that will "clean up" digital threats	
Neutral	
Negative: we have them because we have to, but they can be a hassle at times	
Base	

Total	US	UK
75.8%	79%	72.5%
20.8%	17.5%	24%
3.5%	3.5%	3.5%
0%	0%	0%
400	200	200

This shows that CEOs and the rest of the board need to go further to show CISOs that they are valued. Couple this with how the board sees the inevitability of data breaches, and that 41% of business leads claim to be lacking talent, perhaps it's time that the board started showing the CISOs and other senior security team members just how valuable they are, and actually listen to their advice. After all, these are the experts. They are the people that won't simply let a piece of software dictate their response to a threat: they are strategic, they know the landscape, and they know the enemy.



In summary

For me, this research has thrown up the good, the bad and the ugly. First of all, the good: I am delighted, and somewhat relieved, that business leaders are pretty much unanimously aligned on the fact that cyber attacks are a matter of inevitability. Accepting that there is a real threat is the first step to protecting any business.

It's also great to see an overwhelming dedication to keeping customer and client data safe. Hopefully this means that businesses are taking the necessary steps outlined by this research to prevent any sort of data leakage.

The bad, however, is the confusion over accountability at the top, which is vital. There's a clear split about who should actually take responsibility in the case of a data breach or cyber attack, and this is detrimental to the safety and security of any business. Without a clear chain of command in the event of a cyber attack, the business will lack direction. It's only natural for the CEO to want to take control, but given the apparent knowledge gaps at the top of the chain, it may be time for the CEO and the rest of the board to hand over the reins to the CISO, or equivalent senior person.

Where it gets ugly is how CISOs feel within their organisations. There's a clear disconnect between how valued they feel, and how valued they actually are. Whether that's CISOs misunderstanding how important they are, or the board failing to communicate this to them is hard to say.

What is abundantly clear is that there's still a lot of work to be done. Boards and CISOs need to sit down and agree exactly what the responsibility of the CISO is, and exactly who's in charge of the response to the pervasive cyber threat.

We already know that CISOs are doing their job under the Sword of Damocles; afraid that one slip up could cost them their job. This is something that as a group of business leaders, we need to change.

Boards that can take onboard the feedback of their security experts and begin to hand over control of their business' security posture to those best equipped to do so will find themselves better protected, with a clear process in place should the worst happen.

Aside from the financial investment to match the scale of the challenge, attracting and retaining staff and boosting awareness at the very top of the organisation is key.

Failure to do so could lead to a nasty clash of heads, with a disjointed response to something that is becoming inevitable. I for one hope that is not the case.

- Russell Haworth, CEO, Nominet

Nominet Cyber Solutions

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.

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.com/ntx.

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.

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 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 £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 U.S.

Please note that all figures have been rounded to the closest decimal point for simplicity of reporting.





NOMINET



NOMINET
CYBER
SECURITY

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