The dark side of cybersecurity

The impact on cybersecurity professionals of working blindfolded in an increasingly hostile environment

green raven limited

December 2024

Contents

Introduction

In the physical world, state security services work tirelessly to protect us all from attack, most visibly in the form of terrorism. In doing so, intelligence is critical to their success; it's intelligence that enables them to understand from where attacks are likely to come and/or where they are likely to take place.

In turn, this knowledge enables the security services to take pre-emptive steps to prevent such an attack. And, in the physical world, the intelligence on which the security services depend is highly accurate: published figures indicate that an overwhelming majority of threats are neutralised, and that our security services are blindsided remarkably rarely.

There are clear parallels with the work of cybersecurity professionals and the organisations they protect – not least that being blindsided by the cyberattack that wasn't even imagined is the nightmare scenario and can be the one that does most damage.

But, in cybersecurity, there are also differences. Is the concept of being blindsided even valid when insufficient/inadequate intelligence means cybersecurity teams don't really know to look for threats in the first place? When operating with a blindfold on, literally everywhere could be a blind spot ripe for exploitation by bad actors.

We at Green Raven are firmly focused on how predictive cyber threat intelligence can improve the odds for cybersecurity professionals and the organisations they protect. And in this survey-led report we outline why, by identifying and highlighting:

- the pressure experienced by cybersecurity professionals due to working blind, and its impact on them
- the pressure to justify their budgets, and the difficulty in doing so
- the sustainability or otherwise of current cybersecurity strategies
- the hopes of cybersecurity professionals for AI to tilt the playing field back in the defenders' favour

I'm not sure that "Enjoy" is an appropriate exhortation at this point, given what I already know about the results and what you're about to find out. Nonetheless, we hope you find it enlightening – like removing a blindfold.

Morten Mjels
CEO, Green Raven Limited

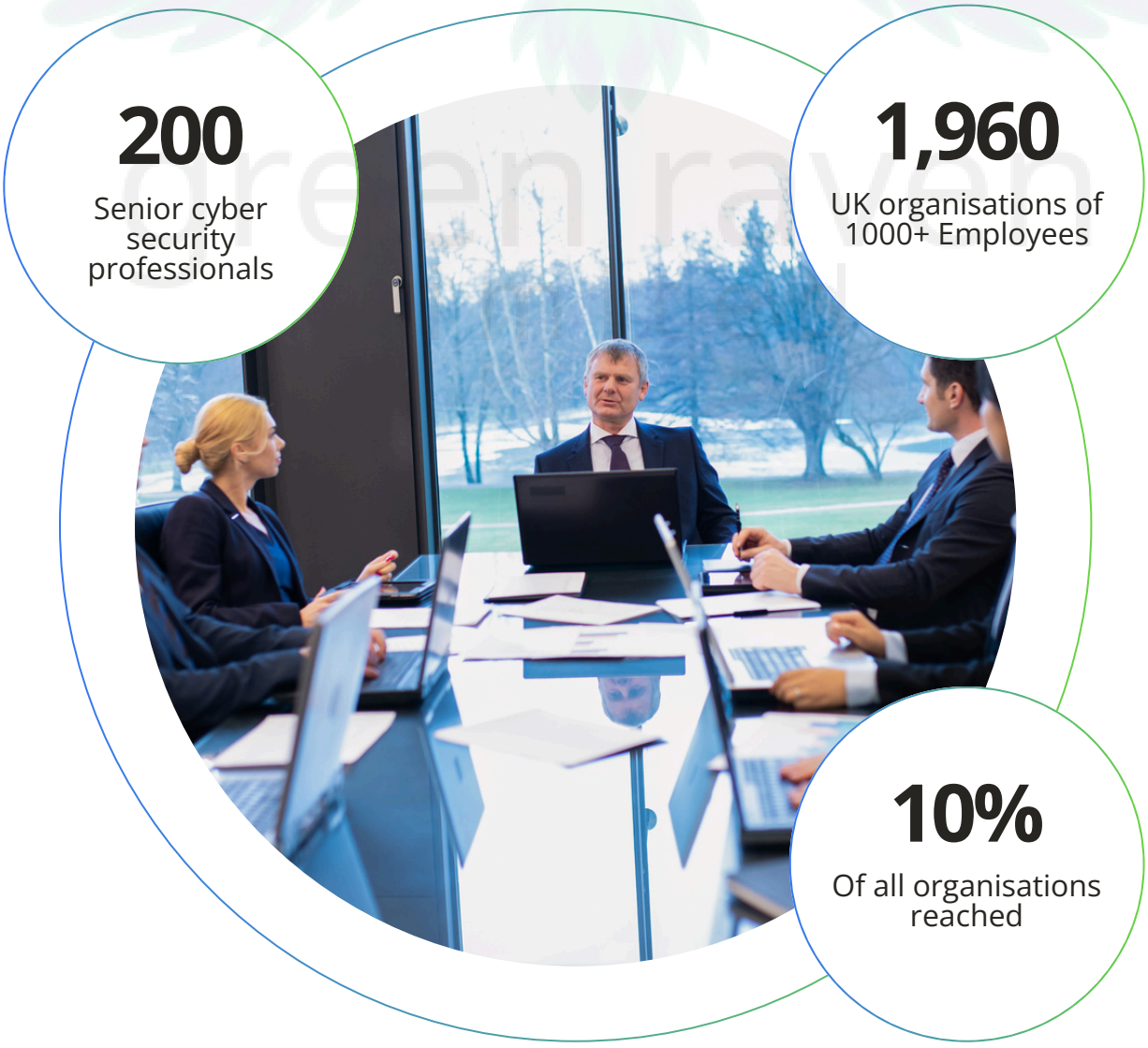
Respondent profiles and survey methodology

Green Raven Limited commissioned research specialists Censuswide to survey:

- 200 senior cybersecurity professionals describing themselves as CISO/director/head/manager of their organisation's cybersecurity team.
- UK organisations with at least 1000 employees.

There are 1,960 organisations in the UK that employ at least 1000 people. This means that this survey reached more than 10% of all organisations in scope.

The survey was conducted at the end of October 2024.



Survey details

Pressure from the job

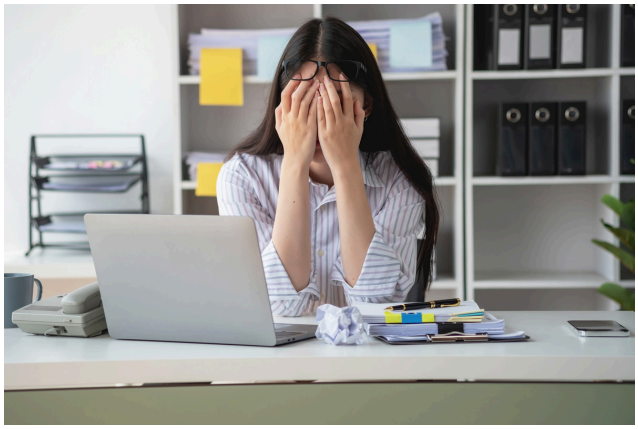
Doing the job blindfolded

The UK Cyber Security Council is responsible for setting industry standards and awarding professional titles for those working in the cyber profession. Cyber threat intelligence is one of the 15 cybersecurity specialisms the Council identifies. It defines cyber threat intelligence as:

"...the assessment, validation and reporting of information on current and potential cyber threats to maintain an organisation's situational awareness."

And the mighty challenge posed by cybersecurity professionals engaged in threat intelligence is encapsulated in a single data point captured by our survey:

67% of respondents agree that "not knowing from where the next cyberattack will come feels like permanently working blindfolded". Barely one in six respondents disagree.



Taking it personally and taking it home

Work-related stress is far from uncommon: an August 2024 survey* revealed that 30% of UK adults find their work in general to be a source of stress. Our research reveals that the current challenges of working in cybersecurity bring significantly higher-than-typical pressures:

Almost 75% of respondents would consider a major breach as a personal failure. And 59% of respondents agree that it's a matter of "when, not if" their organisation endures loss due to a cybersecurity breach"

70% of respondents admit to feelings of professional despair or helplessness at the inexorable rise in cyber losses

However, the standout statistic revealed by the survey is that:

Almost 60% of respondents say that feelings of professional despair or helplessness have a negative impact on their personal lives and/or mental health.
Only one-quarter of respondents said that there was no impact.

*Workplace stress statistics in the UK in 2024

Our view

At a time when there is, even globally, a significant shortfall between the number of cybersecurity professionals needed and the number of cybersecurity professionals working, excess pressure experienced by cybersecurity staff should be a red flag for organisations: such pressure is unlikely to help attract people into the profession or help an organisation retain them.

The onus is on cybersecurity professionals and the organisations that employ them to invest in training and solutions that help turn the odds back in the defenders' favour, easing the sense among cybersecurity professionals that they permanently have their backs-to-the-wall.

But our conversations with prospects and customers – which take place outside the official scope of this survey – strongly suggest that this responsibility may be being dodged, by both cyber professionals and senior management. Even in large companies, cybersecurity is frequently viewed and conducted as a tick-box exercise, with efforts made only to ensure compliance with the minimum requirements of their own customers.

Awareness that this is the case adds to the pressure felt by cybersecurity teams.

The difficulty of justifying budgets

Justifying a 'zero' is always hard

Every department in any organisation needs to be able to justify its existence, activities, headcount, investments and costs, with return on investment (ROI) a common metric in respect of investments in particular.

But ROI is particularly difficult to calculate when cybersecurity investments are designed to prevent loss: how can it be meaningful in its originally intended sense when nothing – which was the goal all along – happened?

This challenge is apparent in the survey results:

Overall, 52.5% of respondents struggle to justify to senior management their level of cybersecurity investment against the actual risks and threats they face

And justifying a 'zero' is getting harder

Amid generally rising cybersecurity budgets:

Almost 70% of respondents feel under pressure from senior management/boards to better justify their level of cybersecurity investment against the actual risks and threats they face

Among those under pressure to improve their justification for their level of cybersecurity investment, a higher proportion – 66%, versus 52.5% of all respondents – say they struggle to justify their level of cybersecurity investment. This suggests that increasing scrutiny does not really mean there are more precise ways of justifying investment.

90%

Say cybersecurity budgets are increasing

Our view

Almost 90% of our respondents also report that their cybersecurity budgets are increasing – a majority of whom reported that budgets were increasing "quickly". (Over half of respondents do not believe their organisation is investing sufficiently.)

Given rapidly rising budgets, the apparent increase in scrutiny from senior management may indicate sensible management/good governance, rather than scepticism.

52.5%

Struggle to justify investment in cyber security

The sustainability of current cybersecurity strategies

Budgets: keeping pace with risks and threats, or not?

Cybersecurity budgets continue to rise:

90% of respondents also report that their cybersecurity budgets are increasing, a majority of whom reported that budgets were increasing "quickly".

Additionally, over half of respondents do not believe their organisation is investing sufficiently given the risks and threats they face.

Despite this, a majority of respondents acknowledge that their efforts will, ultimately, be in vain:

59% of respondents agree that it's "a matter of when, not if" their organisation suffers loss due to a cybersecurity breach

Together, these responses beg the question as to whether current cybersecurity strategies are sustainable, either financially or in terms of their effectiveness. In the view of respondents, however, the answer to this question is, broadly, yes:

Almost two-thirds of respondents say current strategies are sustainable; fewer than one-sixth say current strategies are not sustainable

What are "current strategies"?

The **"gold standard"** formal process for risk and compliance management comprises four-steps: identification, assessment, treatment and monitoring. Almost 80% of survey respondents recognised and acknowledged this long-standing truism. Furthermore:

75% of respondents say that their organisation scrupulously adheres to the gold standard, four-step process of 'identification, assessment, treatment, monitoring' for risk and compliance management.

75%
Say they adhere to the "4 step gold standard process"

Of the remaining 25%:

- fewer than half said that their organisation's process(es) differed substantively from the gold standard
- just over half admitted that their organisation's approach comprised scrutinising risks and applying defensive measures
- two thirds said they used more than one process for risk and compliance management

59%
"**When** not If" their organisation suffer a cybersecurity breach

Our view

A critical perception gap

In respect of current approaches to cybersecurity, there is – worryingly – a substantial majority of respondents that believes it is doing (a) the right thing and (b) doing things right. But there is a distinct divergence between what our survey respondents say and what we observe at most prospects and customers.

What we frequently see 'in the field' is that most approaches, processes and technology solutions – developed over the past decade and currently used by these same organisations – are akin to a two-and-a-half step process that, ultimately, emphasises defensive measures.

For many organisations, a more accurate description of their strategy is to:

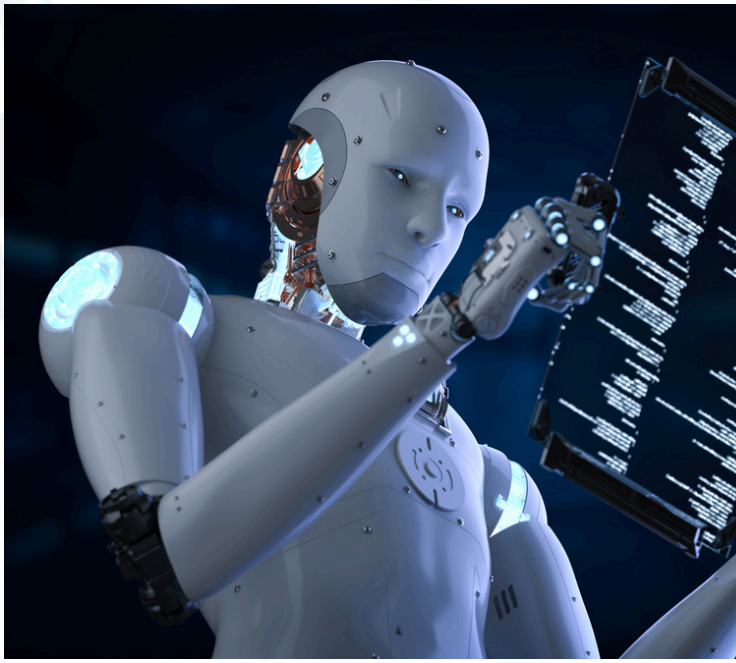
- skip worrying from where the next attack will come (despite the consequence of cybersecurity teams feeling as though they are working blindfold, with all that entails); and, instead
- build ever-higher walls around the organisation's digital estate, hoping that these will be sufficient to keep out attackers (or, at least, to persuade attackers to switch their attention to a more vulnerable target)

What does this mean?

If cybersecurity professionals believe their current approaches are sustainable – even if they also acknowledge that evidence of their effectiveness suggests otherwise – then this presents a severe challenge in terms of changing expectations. The challenge is especially acute because the current status quo and attitudes have taken a decade to evolve; they are ingrained and entrenched.

What might trigger such a change?

In the following section, we will look at some possible reasons.



AI: a new champion

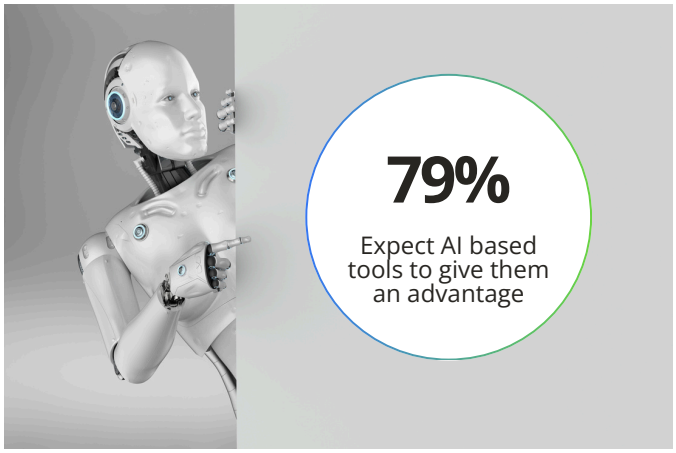
One potential answer to the question posed at the end of the previous section is Artificial Intelligence (AI).

In our survey, we measured the extent to which cybersecurity professionals hope that AI will tilt the playing field back in their favour:

79% of respondents expect new/emerging, AI-enhanced tools to provide them with a GENERAL advantage over threat actors. Not a single respondent strongly disagreed.

We asked specifically how AI could help them to revise their strategy from building ever-higher defensive walls to reinforcing defences where we believe they are about to be needed. Responses to this followed a very similar pattern:

79% of respondent expect new/emerging, AI-enhanced tools to provide me with an advantage over threat actors in respect of BETTER CYBER THREAT INTELLIGENCE



Our view

Clearly, respondents know that bad actors will also have AI-enabled tools at their disposal. So a possible interpretation of the data is that cybersecurity professionals anticipate new/emerging AI-enabled tools for cyber attack and cyber defence to effectively cancel each other out, in a way that current offensive/defensive tools do not.

In respect of the advantage that AI-powered cyber threat intelligence tools can provide, respondents are certainly on the right track. AI-powered cyber threat intelligence tools promise to transform many of the metrics explored earlier in this survey, including:

- reducing the sensation of working blindfolded, uncertain of from where the next attack will come
- addressing the feelings of personal responsibility for breaches
- reconnecting cybersecurity investment levels with the risks and threats actually faced
- fully restoring the gold standard, four-step process for risk and compliance management and make it – re-make it – the norm
- reducing the proportion of cyber security professionals who expect, in the end, defences to be breached, by tilting the table back in favour of the defence

Conclusions

Current cybersecurity assessments predominantly inquire about the strength of defences. This is natural: organisations are primarily concerned with protecting against unknown threats, so the strength of the defence becomes the focus.

Consequently, the standard approach to cybersecurity is to throw vast resources at building what amounts to a metaphorical tall wall around assets, uniformly. Faced with new or emerging threats, we simply add layers to our metaphorical wall – meaning, in the real world, bolt-on solutions and reactive measures. There's nothing 'surgical' about it.

But this approach isn't working. As this survey shows:

- the pressure on cybersecurity professionals is, as this survey shows, increasing to intolerable levels
- budgets are rising and already difficult to justify to those paying the bills
- there may have been a loss of understanding over the last decade in respect of best practice for risk and compliance management

Additionally, existing figures for the number of attacks and the value of losses sustained speak for themselves.

The situation is, in every sense, escalating. A fundamental shift in strategy and a move towards a more comprehensive and proactive approach are both, urgently, required.

Many organisations allocate a fixed budget for cybersecurity defence without a thorough risk identification process. They allocate funds to areas recommended by external sources without truly understanding their specific risks.

There is another way, which helps to streamline cybersecurity and reconnects your cybersecurity budget with the risks and threats you face – easing the route away from the traditional (and expensive) throw-money-at-all-of-it-and-hope-something-sticks approach. Green Raven is committed to the white-labelling and integration of cutting-edge solutions that provide precise, real-time understanding of the risks and threats an organisation faces, enabling them to target resources at constructing efficient, effective defences where they are needed.

To extend the defensive wall analogy, this means adding defensive measures at those points where there are warning signs – intelligence – indicating that an attack is going to come. While this is the essential purpose of cyber threat intelligence, Green Raven's approach aims to take its execution to a new level, with AI-powered solutions able to detect threats that others can't.

Read more about our solutions here, or contact us for more information.

About Green Raven Limited

Based in Cheltenham, UK, and covering EMEA and the Nordics, Green Raven Limited is a specialist cybersecurity consultancy and reseller, applying decades of track record, experience and knowledge to bring together customers and cybersecurity solution providers. In particular, Green Raven is a white-label partner for Darkscope, the world's premier predictive cyber threat intelligence for enterprises.

Green Raven's implementation of Darkscope's unique, award-winning, AI-powered portfolio of solutions spots cyberattacks that others can't, and before they take place – so those responsible for cybersecurity can reinforce their cyber defences where they know they're about to be needed.

Contact

Use any of the contact details below to discuss the results in more detail.

Please credit/acknowledge Green Raven Limited as the source when quoting from this report.

Green Raven Limited

Hub 8
Cheltenham
Gloucestershire
GL51 7SJ, UK

Contact

Phone

+44 (0) 1242 43 00 43

Email

info@greenravenlimited.com

Website

www.greenravenlimited.com