VOICE OF SECOPS, 3RD EDITION 2022

Why your cybersecurity leaders and staff are thinking about leaving

SURVEY REPORT

www.deepinstinct.com

Table of contents

Introduction

Deep Instinct recently commissioned research to better understand and quantify the causes and impact of stress on the cybersecurity community. The research confirms what many in the industry have long known — that stress on Security Operations staff is acute and growing more problematic. Long term, this has the potential to have considerable ramification for the cybersecurity readiness of organizations across the globe.

- More than 90% of cybersecurity professionals are stressed in their role
- Nearly half of the respondents (46%) have thought about quitting the industry
- Stress levels are increasing across all sectors
- The more senior the cybersecurity role, the more stressful the job
- A significant proportion of professionals concede that stress is negatively impacting their ability to do their job
- There appears to be a widespread adoption of completely counter-productive measures, such as switching off alerts because SecOps teams find them overwhelming
- Paying off the ransomware scammers in the aftermath of an attack results in trouble-free consequences in just 16% of cases

We've identified that *more cybersecurity professionals than ever are seriously considering leaving the industry permanently as a result of these pressures* - with potentially catastrophic consequences for the organizations that rely on their vigilance.

This report provides insights into the causes and impacts of those stresses and also lays out some practical solutions that forward-looking organizations can adopt in to improve their security postures and cyber readiness.

"We are too reliant on the hero mentality – we have some people who are working 16-18 hour days at times. That's not sustainable, and we certainly shouldn't be expecting people to put in those kinds of shifts as a part of our capability. They'll burn out."

– UK-based CISO at a large police force

"The number of unknowns is increasing. The criminals know their existing malware signatures can be detected, so they are constantly looking to find new ways to attack. It's like they've got Harry Potter's invisibility cloak. We can never switch off."

– US-based Divisional Head of Cybersecurity Compliance, major global motor manufacturer

Management summary

The pandemic has caused dramatic impacts to our work and home lives. Many of us are still sorting its impacts. And due to the nature and importance of their work in securing information systems from compromise, the SecOps community was as impacted as much – if not more – by the stress of the pandemic as any discipline.

For CISOs, the following areas have been recognized as the top stressors:

- Managing security for a remote workforce
- Digital transformation and its broad impacts on security posture
- Ransomware threats

For SecOps practitioners, key stresses include:

- Insufficient SecOps staff to fully meet security needs
- The impossibility of preventing all threats (with the expectation by senior leaders that this is even possible)
- Long work hours with the need to always be on call / available
- Inadequacy of the existing solutions stack

SecOps teams are clearly struggling with many priorities in the face of unprecedented challenges.

With workforces still fully remote – and with many remaining in this standing permanently – the work of securing endpoints and the overall environment will be no easy task, especially for enterprise organizations. The pandemic ushered in a new era of work and even after two years the strategies for securing remote and hybrid organizations are still evolving.

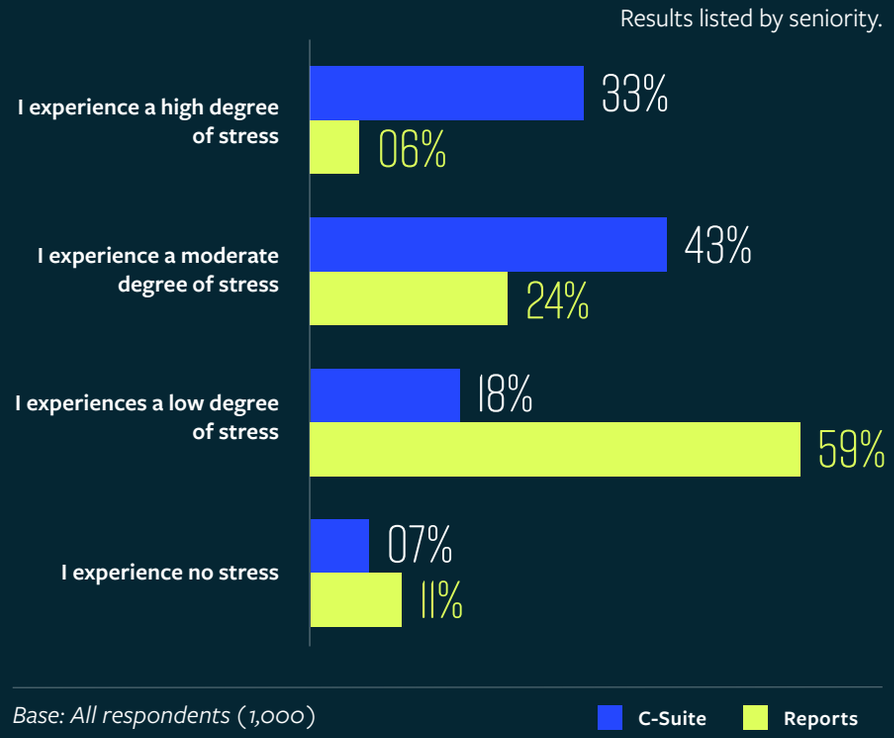
These challenges significantly contribute to rising stress levels and are prompting highly skilled SecOps professionals to leave or consider leaving the industry at all levels, but particularly at the C-Suite level.

To combat this problem, the industry must look for new ways to reduce employee fatigue and burnout and reduce staff churn. Finding ways to automate processes that lessen workloads, improve quality of work, and raise job satisfaction is a top priority.

Key criteria towards this endeavour includes the following:

- Lowering false positives to raise the quality of the work
- Implementing more preventive measures that allow security pros to catch threats earlier and relieve stress
- Improving investigation and response times to improve security posture

Who is stressed, and how much?



91% of the cybersecurity professionals in our survey claimed to be experiencing some level of stress, and almost 1 in 5 of those surveyed claimed to be "highly stressed."

However, the largest overall cohort of "highly stressed" executives were those at C-Suite level: one in three C-Suite execs surveyed (including CISOs, ITOs, CTOs, Global IT Strategy Directors) claimed to be "highly stressed," compared to 6% of their reports making the same claim.

Overall, stress levels among cybersecurity professionals are growing higher over time.

When we asked professionals claiming to have any level of stress whether levels had risen or fallen in the past 12 months, respondents were nearly twice as likely to claim their stress levels had risen (46%) than had fallen (26%).

These trends have been echoed in qualitative research undertaken as a part of this project:

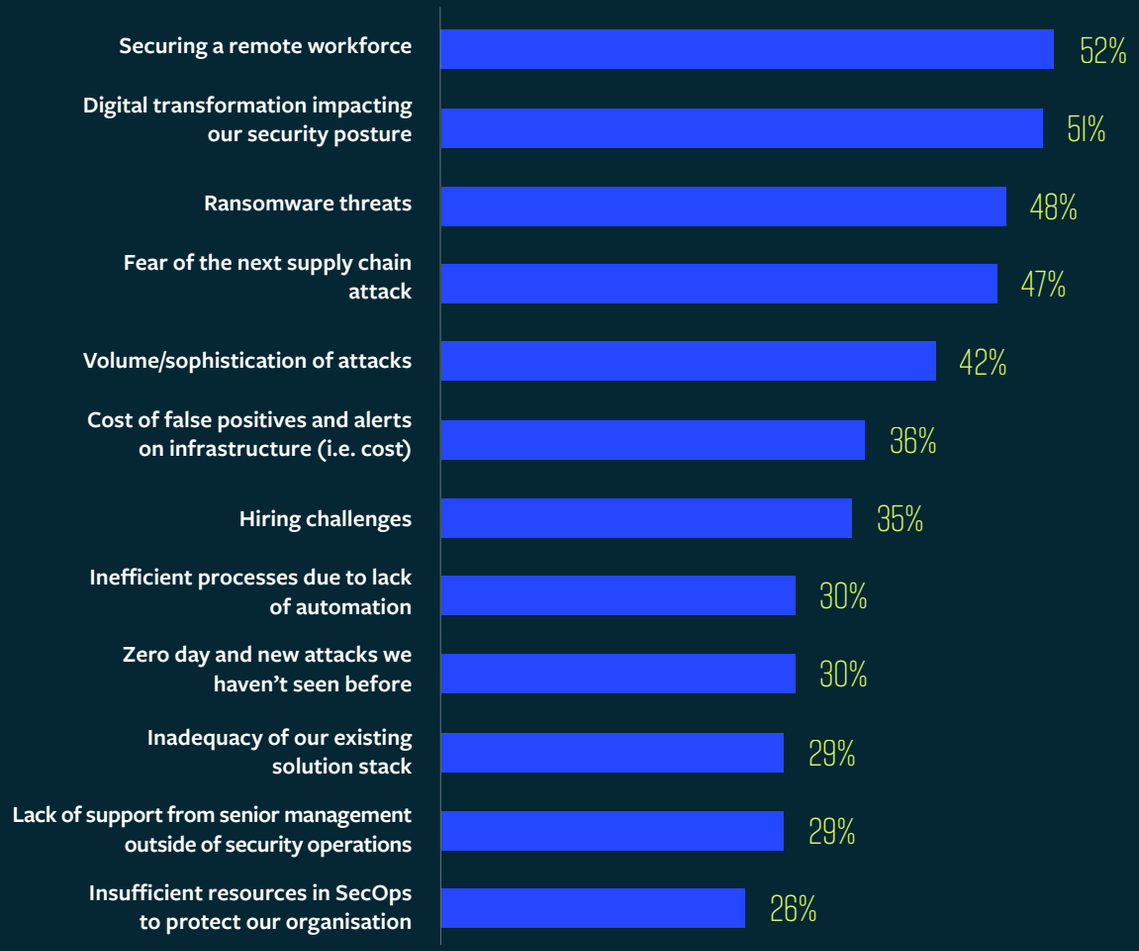
"I think the pressure of failure is significant, it's stressful for a lot of people... it's always easy to blame the security team for a hole in the security posture that has actually been exposed by a human in an entirely different department clicking on a link in the face of all the training and advice that the cyber defence people have set out... and the SecOps staff get it in the neck when they are working stupid hours to try and keep the ship watertight."

– US-based public sector CIO with Cybersec responsibility for county with 1.5m citizens

"People are under more stress because of COVID. They rely more on their home routers, home network. The attack surface has expanded exponentially."

– CISO, German-based international healthcare group operating over 50 healthcare centres

Specific pressures for the cyber C-Suite



Base: C-Suite respondents experiencing some degree of stress (467)

The root causes of the rising stress levels are varied and tend to be different compared to those impacting their reports.

From a list of 12 potential stress causes provided to respondents, the top three were:

- Securing a remote workforce (identified as a stress root cause by 52% of stressed C-Suite respondents, rising to 60% of C-Suite execs claiming to be "highly stressed")
- Digital transformation impacting security posture (51%)
- Ransomware threats (48%)

It is interesting that COVID-related challenge of securing a remote workforce remains a significant stress cause two years after pandemic first emerged. Digital transformation as a close second signifies the challenge of securing hybrid environments. And ransomware at number three talks to the real pressure organizations feel to protect against this very damaging and costly threat.

This tells us that the stress levels identified amongst the cybersecurity C-Suite are not transient, and there is potential for those stresses to rise further unless ways can be found to mitigate them.

"There are so many 'unknown unknowns' in this industry. We have to be permanently on our toes. Sitting back and waiting to be hit is not an option. Lives are at risk as well as businesses."

– CISO for US Healthcare Group managing 20 hospitals

Specific challenges for SecOps teams

For cybersecurity execs reporting into the C-Suite, there are a different set of stress factors.

Chief among them:

- It is impossible to stop every threat, yet expected (cited by 47% of stressed direct reports)
- Expectation to always be on call / available (43% of stressed direct reports)
- Inadequacy of our existing solutions stack (40%)
- Insufficient SecOps staff to do the role properly (40%)

Typically, each respondent identified 3 to 4 different stress causes.

> "If you CAN prevent even 95% of attacks that relieves massive pressure on the team you've currently got flailing around trying to neutralise all the incursions – often imagined rather than real, I might add – that the detection applications are picking up."
>
> **– CISO for major US domestic mortgage lender**

Key threat fears summary

To better understand the key external threats at the root of these stresses, we asked respondents to choose the single threat they considered to be the most significant.

The results show there is not one clear winner which reinforces why stress levels are so high. Without a singular focus on one type of attack, resources are stretched thin and its obvious to see how a SecOps team may feel deflated against the challenges they face.

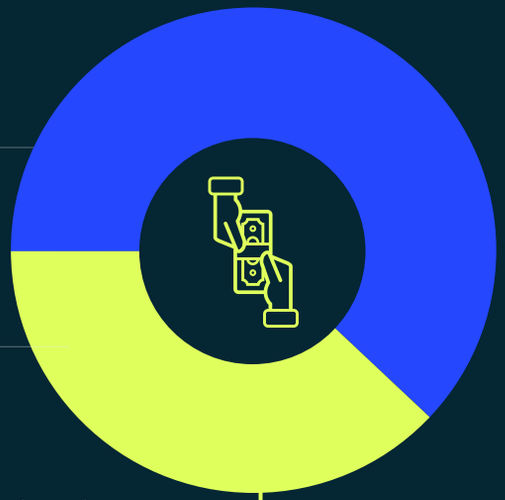
Base: All respondents (1,000)

Ransomware – the universal threat

Of all the external cybersecurity threats identified, ransomware appears as a top 3 concern in almost every country, vertical, and level of seniority we surveyed.

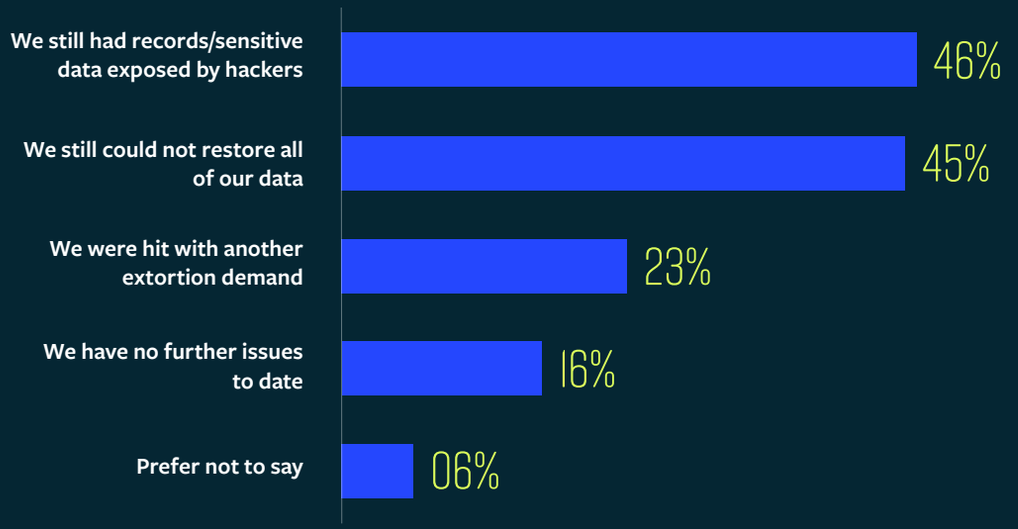
This is hardly surprising, given 38% of survey respondents admitted to both experiencing a ransomware attack, and paying the ransom - with French (56%) and German (51%) respondents the most likely to have paid out.

Percentage that paid



Base: All respondents (1,000)

What happened to those that paid?

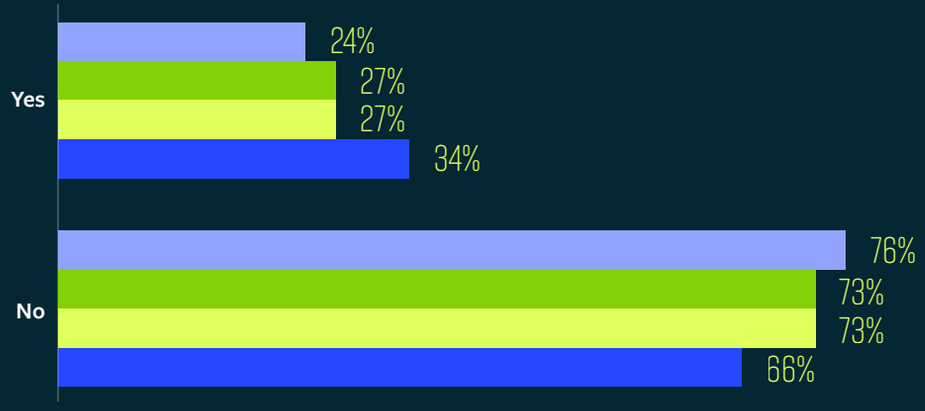


Base: Respondents who paid the ransom (377)

Yet despite the above findings, around 1 in 4 respondents still believe they would pay a ransom in the event of a future ransomware attack.

Percentage that would pay again in the future

Results listed by country.



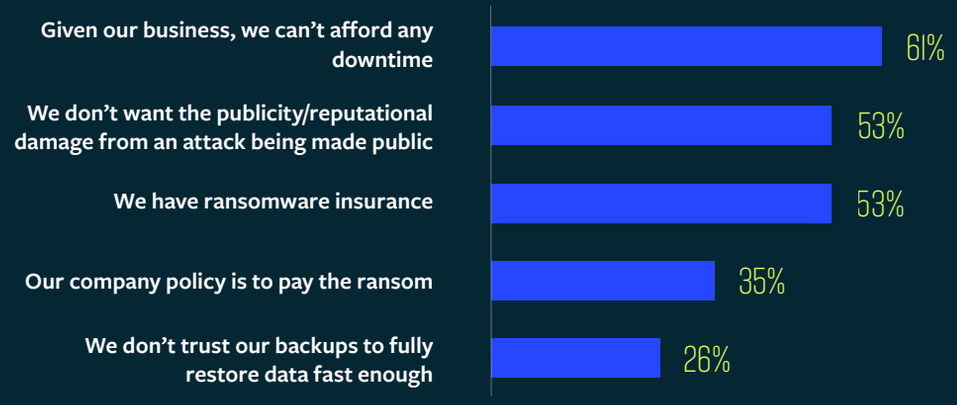
Base: All respondents (1,000)

US UK France Germany

Interestingly, despite the large sample size, there appeared to be no significant differences between respondents in different verticals – respondents in healthcare were statistically no more likely to pay up (or not) than those in Critical Infrastructure or Technology or Retail & E-commerce, for example.

Why might they pay in the future?

When asked, "why pay?" there were a variety of reasons given. "Downtime avoidance" was the most common answer (61%). Reputational issues were a significant factor as well, with more than half (53%) citing this as an issue.



Base: Respondents who would pay the ransom (266)

"Ransomware to many is still the 'it won't happen to me' kind of approach."

"A lot of manufacturers are not properly prepared to repel ransomware attacks, or deal with the consequences – not just in terms of finding the ransom money, but in terms of actually resetting their business to a stable state afterwards".

– US-based Head of Cybersecurity, industrial electrical components manufacturer

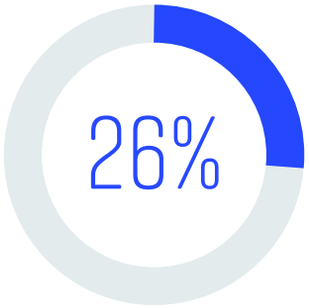
Stress – the role of false positives

The volume and time-intensive nature of addressing false positive alerts was a critical stressor for respondents.

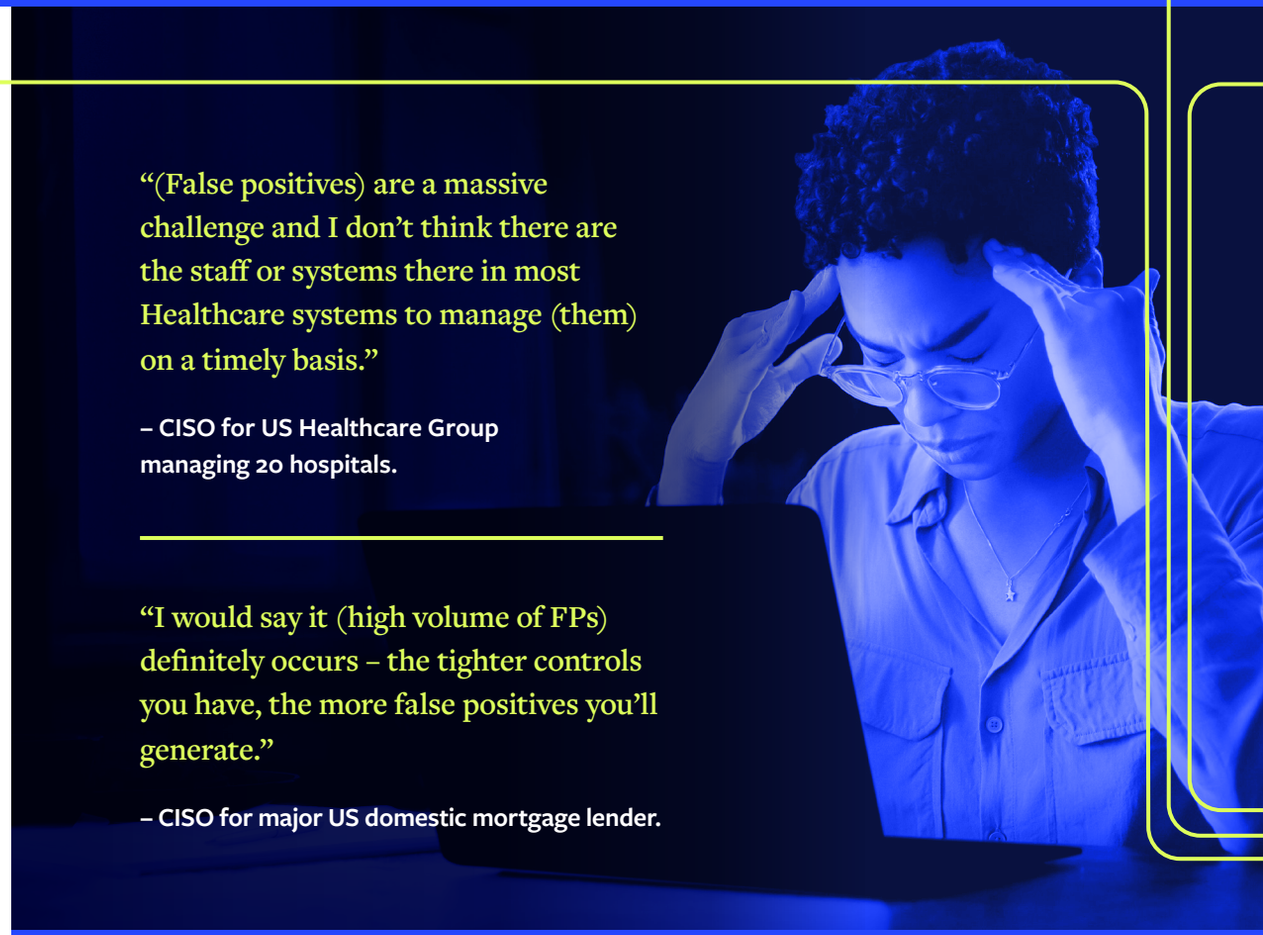
74% claimed their volume of false positive was *steady* or rising (to 83% in Germany).

C-Suite respondents were markedly less likely than their reports to see the significance of the challenge, further underscoring the divide between leaders and their direct reports. 36% of C-Suite respondents thought their false positive rate was in decline, but only 19% of their reports – the people largely charged with dealing with them – reported this was actually the case.

Perhaps of greater concern, though, is that when we asked those with steady or rising false positive incidence rates, more than 1 in 4 respondents (26%) confessed that they actually "turn off our alerts because they are too noisy."



More than 1 in 4 respondents (26% of those respondents with steady or increasing false positive rates) confessed that they actually **"turn off our alerts because they are too noisy."**



"(False positives) are a massive challenge and I don't think there are the staff or systems there in most Healthcare systems to manage (them) on a timely basis."

– CISO for US Healthcare Group managing 20 hospitals.

"I would say it (high volume of FPs) definitely occurs – the tighter controls you have, the more false positives you'll generate."

– CISO for major US domestic mortgage lender.

"Right now, we are employing 60 to 70% extra staff because of false positives."

– US-based CIO of bank with over 1000 branches worldwide

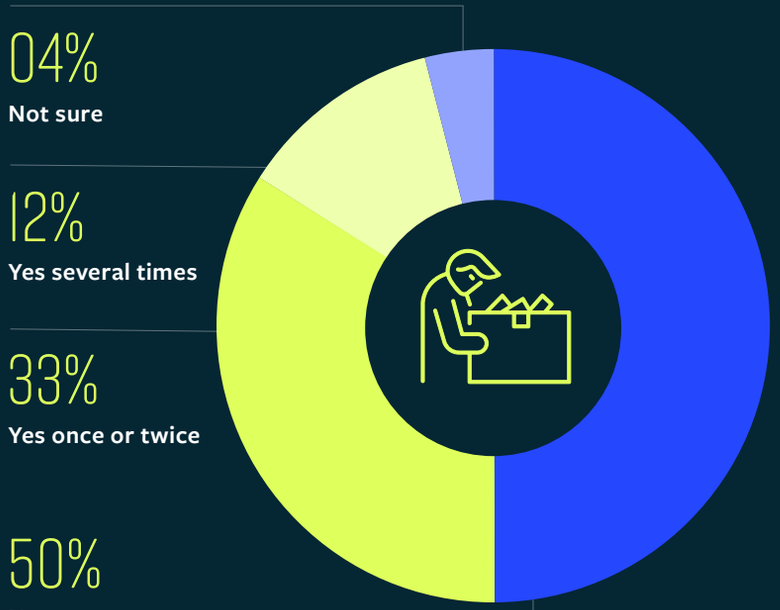
The SecOps workforce – and the great resignation

So how are cybersecurity professionals coping with these stresses?

For many, the answer is "not at all well" and many are considering leaving the cybersecurity industry altogether as a result of this stress. 45% of respondents experiencing some stress level claimed that work stress has led them to consider leaving the cybersecurity industry on at least one occasion. (To be clear: that's not just leaving their employer – that's leaving the cybersecurity industry altogether).

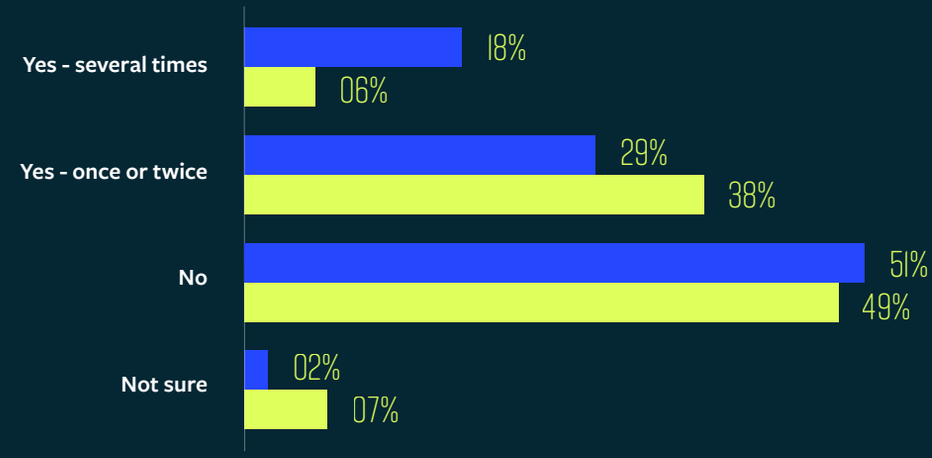
At a time when it is a challenge to fill all of the open roles in cybersecurity, estimated to be 465,000 in the US alone, these statistics are very concerning.*

Have cybersecurity professionals considered leaving the field due to work related stress?



Base: Respondents experiencing some degree of stress (913)

Stressed C-Suite respondents (18%) are three times more likely than their reports (6%) to have considered leaving the industry "several times."



Base: Respondents experiencing some degree of stress (913) C-Suite Reports

Of course, these results are only from execs who have remained in the industry despite the pressures. In our survey 46% of respondents claimed to know of at least one peer who has already left the industry altogether due to stress.

*Cybercrime Magazine: https://cybersecurityventures.com/jobs/

Making the business case for preventative solutions

Acknowledging the significant negative impact of stress on the effectiveness of SecOps teams is one thing, building the business case for reducing those stresses can be quite another.

Our survey has uncovered several tangible benefits to introducing new solutions that can mitigate the stress impacts and improve overall security operations within organizations.

Respondents were able to identify a significant range of benefits in the event that they were able to half their security incident rate. Among the chief benefits were lowering business risk (62%), protecting data from exfiltration (61%), and saving costs on post-execution investigation (58%).

SOC impact of a 50% incident reduction

Base: All respondents (1,000)

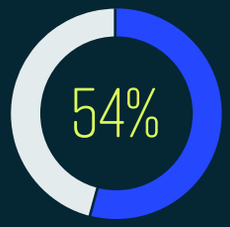
"Prevention-first makes so much sense to me."

– CISO for network of US healthcare centres, over 100 sites in US

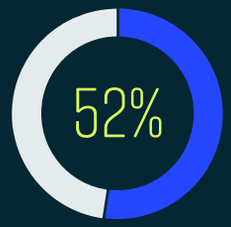
Ransomware prevention cost benefits

When asked how a 50% reduction in incident rates would impact their work, answers were varied, ranging from a reduction in storage costs to the alleviation of demand for more highly skilled analysts.

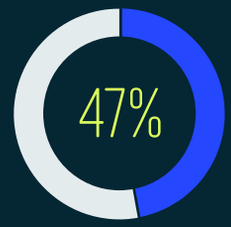
Similarly, respondents identified a wide range of cost-benefits for preventing ransomware, including the following:



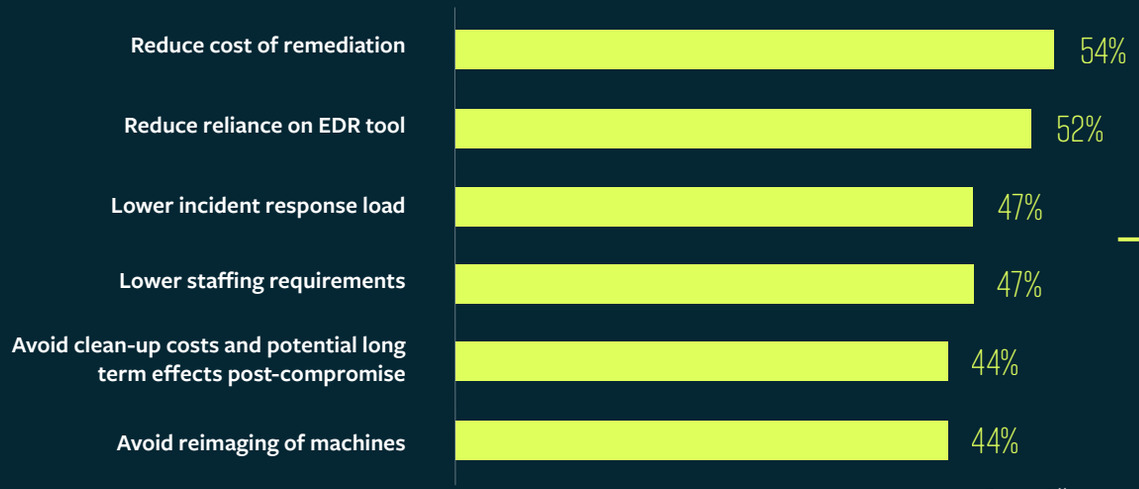
Reduction in mediation costs



Reduction in reliance on EDR tools



Lowering of the organization's incident response workload



Base: All respondents (1,000)

Conclusions

Cybersecurity professionals are under growing pressure to defend their organizations against increasingly creative threat actors and stress levels are rising relentlessly.

Unsurprisingly, the more senior the position, the more stressed the executive. And these executives are stressed because of the increased complexity of the modern workforce and workplace combined with the more advanced (and potentially pain-inducing) threat landscape. It appears that being a senior cybersecurity leader has never been more challenging than today.

Senior cybersecurity executives acknowledge that their stress levels are impacting decision-making and can have implications for the security posture of companies.

The stress we're seeing across the cyber industry appears to be accelerating the exodus of talented people from the industry: a particular challenge when many cybersecurity defenses and mitigation processes are human-dependent, requiring constant monitoring and intervention.

While cyber professionals do believe the tools they need to protect themselves are improving, they also believe much more can be done.

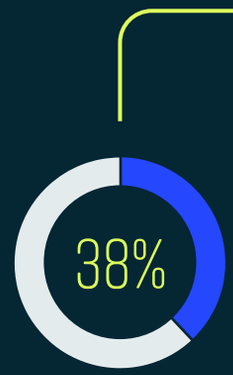
The volume of false positives remains a significant issue for many professionals, impairing SecOps teams' ability to combat cyber threats.

Levels of business risk, data protection levels, and the cost of post-execution remediation would all be positively impacted if false positives could be markedly reduced.

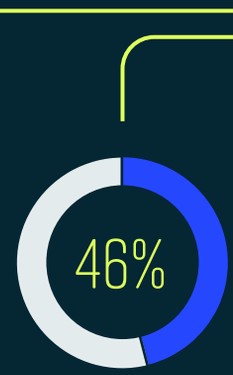
Ransomware is a top-3 threat in every vertical and in every country surveyed.

Ransom payments are more widespread than many may believe. Nearly 4 in 10 (38%) respondents claim to have paid a ransom for return of data / encryption key. But paying the ransom did not solve the issues for many of these respondents. Nearly half (46%) admitted they still had data exposure issues and 45% claimed they could still not restore all their data after paying the ransom.

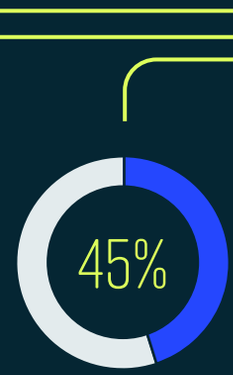
> "I need something that prevents a malware file from being downloaded, rather than something that tells me a file's been downloaded after the event."
>
> **– CISO for network of US healthcare centres, over 100 sites in US**



Nearly 4 in 10 (38%) respondents claim to have paid a ransom for return of data / encryption key



Of those that paid up, nearly half (46%) admitted they still had data exposure issues



Of those that paid up, 45% claimed they could still not restore all their data after paying the ransom

Recommendation

The cybersecurity industry needs an intelligent solution that does the following:

- Dramatically reduces false positive rates - ideally through improved cyber defenses that actively prevent incursion - rather than relying on human-led, post-incursion detection and response to remediate
- Offers robust AI-driven prevention of increasingly creative ransomware attacks that are not always fully mitigated by a ransom being paid
- Helps alleviate staffing issues, stress, and budget challenges that are leading to high staff turnover and apathy within SecOps teams

> "I need a really basic but comprehensive tool that can prevent intrusion rather than have to spend all my time and resources worrying about how a deal with an issue that's already inside my system."
>
> **– CISO for network of US healthcare centres, over 100 sites in US**

Appendix

Respondent base

Quantitative interviews were conducted with 1,000 senior cybersecurity subject matter experts from companies in the USA (500), UK (200), Germany (150) and France (150).

All interviewees worked for businesses with 1,000 employees or more, and for businesses with annual revenues of at least US $500M.

Interviewees came from a broadly representative sample of businesses in Financial Services, Retail & eCommerce, Healthcare, Manufacturing, Public Sector, Critical Infrastructure, and Technology / related advisory businesses.

Typical job roles of interviewees were CISO, CTO, ITO, Chief Security Officer, Head of Information Security, Information & Security Risk Manager, Malware Analyst etc.

All quantitative respondents were screened for having some level of input into the management of information security in their company. Half of the respondents were CISOs or in an equivalent role.

The quantitative survey was supplemented with 12 in-depth qualitative Zoom interviews with US-based and European CISOs in the Financial Services, Healthcare, Manufacturing and Public Sectors, all of whom worked for organisations with annual revenues of at least US$500m.

This report was authored by:

Simon Hayhurst
May 2022
www.hayhurstconsultancy.co.uk

Deep Instinct takes a prevention-first approach to stopping ransomware and other malware using the world's first and only purpose built, deep learning cybersecurity framework. We predict and prevent known, unknown, and zero-day threats in <20 milliseconds, 750X faster than the fastest ransomware can encrypt.

Deep Instinct has >99% zero-day accuracy and promises a <0.1% false positive rate. The Deep Instinct Prevention Platform is an essential addition to every security stack — providing complete, multi-layered protection against threats across hybrid environments.

www.deepinstinct.com | info@deepinstinct.com