ThreatConnect.

Whitepaper

CyberSecurity Under Stress

Introduction

Is cybersecurity broken?

Whether you are in financial services, farming, or public infrastructure, the security threat to organizations has never been greater. Today, almost every company is a technology company in some shape or form and this can be a soft underbelly - open to attack.

Cyber risk is the fastest-growing risk faced by businesses globally. A wide range of statistics and sources make it clear that attackers have become even more proficient over recent years, using automation to exploit vulnerabilities at an accelerated pace and frequency. Threats are even more widespread and complex than before.

Managing risk has put added pressure on cybersecurity teams on a global scale, which increases financial burdens and has human consequences for the people who work in them.

To those on the front line, the accelerating number of cyber attacks, data breaches, and the scale and speed at which threats emerge can sometimes feel insurmountable and infinitely expensive to deal with. Gone are the days when the human resources within security teams alone could 'fix' problems.

As the research in this report highlights, more than ever, SecOps teams are being asked to do more with less, leading to higher stress levels that impact both their work and personal lives. We surveyed over 500 security professionals in both the US and the UK. The growing risk from cyber attacks is also compounded by significant recruitment and retention issues within cybersecurity. Over a quarter of respondents (27%) across the US and UK are considering quitting their jobs in the next six months. Meanwhile, senior decision-makers report an average turnover rate of 20%, and 2 in 3 have seen a notable increase year on year.

While this is no doubt aligned with the "Great Resignation" trend affecting many industries, there are also signs of stress and burnout. This only serves to make the sector less attractive to talent and the problem of long hours, heavy workloads, and understaffing more acute.

This also contributes to one of the most significant issues faced by the industry today: the chronic cyber skills gap in the workforce. It is one of the most common challenges as we head into 2022, with a whopping 45% of IT Directors across the UK and US putting skills and qualifications as the biggest barrier to recruitment. And with 35% citing salary competition, 33% working conditions (e.g., stress and workloads), and 32% work patterns (e.g., long, irregular hours) as barriers to recruitment, it's clear that organizations need to do everything they can to hold on to skilled professionals while upskilling existing staff.

Security as a business strategy

Cybersecurity needs a rethink but is far from being broken. The industry is on a trajectory to make security leadership more business-driven, aligned with all parts of an organization. Every day at ThreatConnect, we see the connection between business value and the security team's value to the business. However, one of the biggest challenges that cybersecurity leaders face today is gaining business buy-in for what needs to be done and the specific initiatives that need to be put in place to protect the organization.

This can be overcome by asking - what is the business looking to do, what are its goals, and how can we support that?

A strong understanding of the business strategy, coupled with IT risk and the ability to map out security requirements, is the fundamental basis for success. Yet, for many businesses, cybersecurity is often the only part of the business where senior leaders need support to understand what 'good' looks like.

Tools of the trade

As the world becomes more connected, the importance of supporting these teams with the right tools and support to get the job done will also increase. The emphasis here is on the word 'right.' So-called 'tool sprawl' can simply drive up costs without contributing to a SecOps team's effectiveness. According to research from the Ponemon Institute[1], the average enterprise is now running 45 different tools and technologies. Still, those that have more than 50 solutions in place are rated 8% less able to detect a cyber attack — and 7% lower in their ability to respond — than organizations using fewer than 50 tools.

Cybersecurity should not become a black hole of investment but rather an integral part of business success. Our goal at ThreatConnect is to help organizations quantify the actual risk of a potential security incident in terms of revenue and financial losses. Cyber risk quantification makes it straightforward for the broader business to understand and address effectively. As practitioners, we continually strive to improve incident response efficiency and effectiveness, making for happier and more productive defenders.

Balaji Yelamanchili

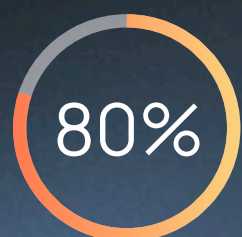**Balaji Yelamanchili**
CEO
ThreatConnect

[1] Security leaders are still in the dark with asset visibility while a lack of insight is driving control failures
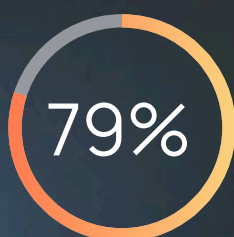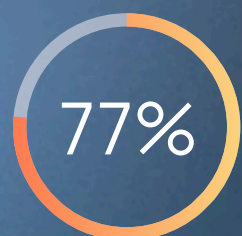
Research Highlights

Cybersecurity Capabilites

80%

say that when it comes to cybersecurity, their company is focused on the right things and understands the most important risks

79%

say that their cybersecurity team/organization can regularly demonstrate its effectiveness and the return on cybersecurity investments

77%

believe the company they work for has the right security systems to defend against complex cybersecurity attacks

74%
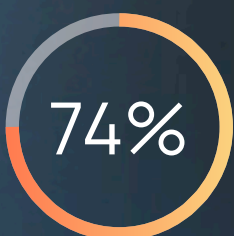
feel the company can keep up with the volume and sophistication of cyber threats

Access to Skills and Talent

The top 3 barriers to recruiting employees with skills in security are:

38%

Finding people with the skills and qualifications required to do the job

34%

Working conditions (e.g., stress, workload)

32%

Work patterns (e.g., long, irregular hours)

Staff Turnover

32%

of IT Managers and

25%

of IT Directors

are considering quitting their jobs in the next six months

The average number of staff with direct responsibility for IT security is

6.85

On average, over the past 12 months, respondents estimated a

20%

staff turnover rate

70%

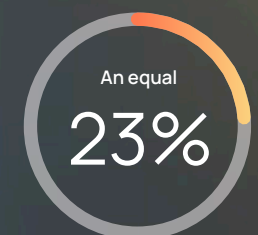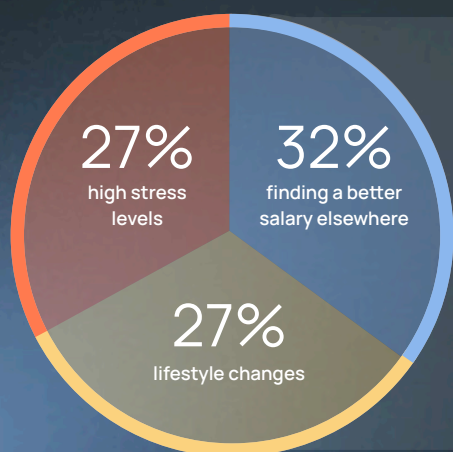of respondents aware of staff turnover say it has increased in the past

12

months

Research Highlights

The Top 3 Reasons Employees Are Leaving Their Current Job

27% high stress levels

32% finding a better salary elsewhere

27% lifestyle changes

An equal **23%** of respondents reported excessive workload, better career prospects elsewhere, and performance issues

Of those planning to quit in the next six months, better salary and better career prospects elsewhere were the two most popular reasons **(30% and 28% respectively)** followed by high stress levels **(27%)**

Workplace Stress

32% of respondents report being very stressed about their current job

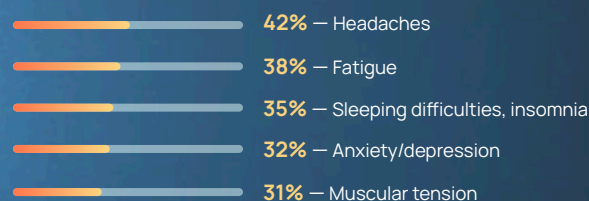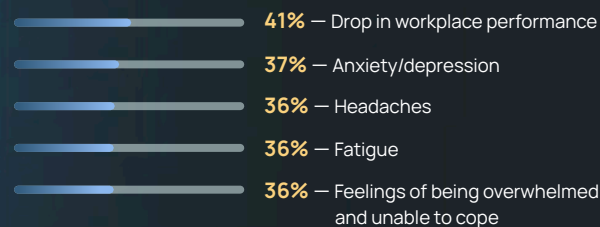**55%** More than half say their stress level has increased in the past six months

The most common causes of stress are heavy workloads (32%), long hours (31%), and tight deadlines (21%). 18% cited a rise in security incidents as another major cause of stress

The Top 5 Reported Work-Related Stress Symptoms Included:

Experienced Personally

- **42%** — Headaches
- **38%** — Fatigue
- **35%** — Sleeping difficulties, insomnia
- **32%** — Anxiety/depression
- **31%** — Muscular tension

Observed in Colleagues

- **41%** — Drop in workplace performance
- **37%** — Anxiety/depression
- **36%** — Headaches
- **36%** — Fatigue
- **36%** — Feelings of being overwhelmed and unable to cope

01

Cyber Attacks:
Defending Against The Dark Arts

Cyber attacks on businesses are growing. The number of data breaches in 2021 soared past 2020's total[2] by October alone, costing companies an average of $4.24 million each[3] and impacting millions of customers worldwide.

Organizations are taking cybersecurity more seriously in the face of the rising threat level. PwC's most recent Annual Global CEO Survey[4] identified that cyber threats have graduated to the top of boardroom concerns in Western Europe and North America. Globally, they are second only to the threat of the pandemic and health crises itself and have leapfrogged other concerns such as over-regulation, trade conflicts, and uncertainties around economic growth.

This level of concern is already translating into a swelling of 2022 cyber budgets, with almost half (44%) of security professionals across the US, APAC, and Europe planning to increase allocation to address cyber risks, according to IDG[5].

But what should the priorities be?

---

[2] The number of data breaches in 2021 has already surpassed last year's total
[3] Cost of a data breach 2022
[4] Reimagining the outcomes that matter
[5] IDG Security Priorities Study

01

Measuring and quantifying risk

Until recently, the concept of putting a specific value rather than just a 'high, medium, or low' approximation of the financial risks posed by cyber threats seemed unrealistic. The threat landscape informs risk, but the scale and complexity of organizations and their IT infrastructures and ecosystems were perceived as too great, even by CISOs.

This has changed. What was previously expected to be a piece of analysis months or years in the making is now possible in a matter of days or weeks. This intelligence-led approach allows businesses to prioritize risks, invest in the right people, and extract the most value from security orchestration, automation, and response (SOAR) tools. SOAR enables teams to build sustainable responses that concentrate resources to have the biggest impact and make their daily workflow more manageable.

02

Third-party risk management

One of the greatest 'known unknowns' for organizations is vendors and partners not having sufficient protection against cyber threats. According to IDG's Security Priority Study[5], while 44% of security incidents in 2021 were caused by an employee falling victim to a phishing scam, unpatched software and security lapses are the second leading cause (27%), followed by misconfiguration of services or systems either on or off-premises (26%).

Thus, the ability to quantify third-party risk and ensure you're not compromised via vendors is key – starting by knowing what data third parties have stored. More than just a game of compliance, only with this accurate visibility can organizations assess the actual risks they are exposed to and work out how to deal with it – or make decisions on what level of risk you are prepared to live with and insure against.

03

Managing vulnerabilities

A big challenge facing cybersecurity professionals has been how to show the value of emergency spending. A severe and widespread vulnerability, such as the recently identified critical Log4Shell flaw in Java-based application error logging component Log4j, requires a CISO to prepare robust plans and secure finds to address it quickly. Failure means leaving the organization open to potential attacks and putting defenders at risk of severe burnout.

As the level and nature of specific threats can now be pinned down and presented in a language that the wider business understands, we will see an acceleration in action to remediate emerging threats. Calculating the cost of not dealing with a problem to justify spending is a much more powerful position to be in.

Similarly, using automated tools to deal with endemic challenges such as phishing emails to quickly identify – in seconds - legitimate threats, dissect their impact and prioritize what needs attention is key to deploying resources efficiently and effectively.

---

[5] IDG Security Priorities Study

02

Human Defenders:
Unsung Heroes Under Pressure

Security professionals are the most valuable resource in the fight against cyber threats, yet they are the most thinly spread. When strength and stability are needed most, our research paints a picture of SecOps teams facing a shortfall in the staff required to provide protection.

We've identified a high level of staff churn, skills shortages, burnout, and even low morale, to the detriment of the image cybersecurity has had as a stable, exciting, even lucrative career choice. Let's take a closer look.

Intensifying stressors

As phishing, malware, DDoS, and other types of attacks become more frequent and widespread; security teams face higher levels of work with the same, or even fewer, resources. According to our research, only 74% say their company can keep up with the volume and sophistication of cyber threats.

This is having a drastic effect on their physical and mental health. Almost a third (32%) of respondents to ThreatConnect's research reported feeling highly stressed about work, and more than half (55%) said their stress levels increased over the past six months alone. Longer hours and heavier workloads are notable drivers of personal stress, manifesting most commonly in headaches (42%), fatigue (38%), and sleeping difficulties (35%). 41% also reported noticing a drop in work performance among colleagues. It's no surprise that IT workers are quitting in their thousands, leaving businesses even more under-resourced to potential attacks.

32% Highly stressed at work

55% Stress levels increased over last 6 months

Rising turnover rates

In 2021, senior decision-makers across the UK and US reported an average IT employee turnover rate of 20%, and more than two-thirds (67%) have seen this rise in the past year. More than a third (32%) of Security Managers say they're considering quitting their jobs in the next six months. Why?

Overall, finding a better salary elsewhere is the most commonly cited factor for people leaving their jobs (32%) and the most popular reason given by those considering quitting in the next six months (30%). However, UK respondents were most likely to be thinking of quitting due to a perceived lack of opportunity to work from home (31%), perhaps influenced by the impact of the pandemic.

Across both countries, high stress levels (27%), excessive workload (23%), and better career prospects elsewhere (23%) also go a long way to explain the 'Great Resignation' trend. And it seems these sentiments are spreading, too— with recruiters now struggling to fill the growing number of IT roles available.

Avg IT staff
turnover of

20%

Causes of The Great Resignation

27%
High Stress Levels

23%
Excessive Workload

23%
Better Prospects Elsewhere
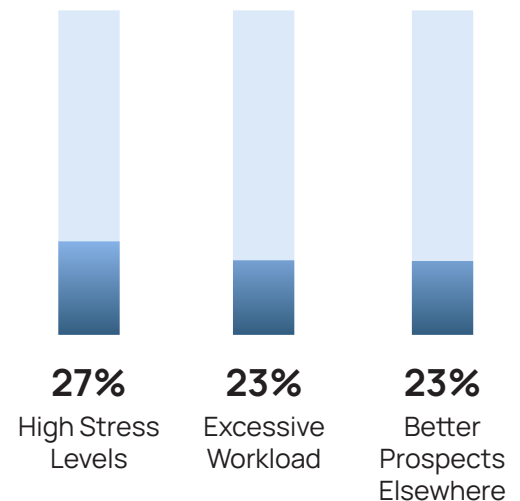
Even harder to hire

More than a third (38%) report difficulties finding people with the required skills and qualifications needed for open roles. However, only a third (33%) of security leaders say they'd recommend a career in IT security to others, with a similar number likely to discourage people from pursuing the profession (33%). This negative view is a significant concern at a time when increasing IT risks and emerging cyber threats will require a highly-skilled, professional and engaged workforce.

Overall, it's clear that unless there are significant changes within businesses and the security profession, companies and their customers are soon likely to face—and fall victim to—even more dangerous cyber attacks.

So, what's gone wrong? What are the splits between business leaders and their IT specialists— and how can they mend their differences to create safer and stronger businesses?
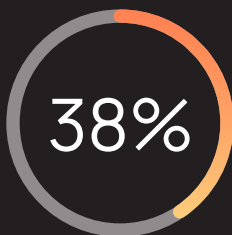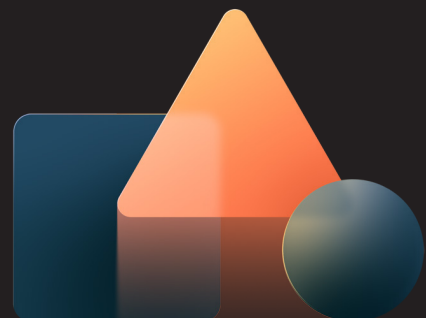
38% Can't find highly skilled professionals
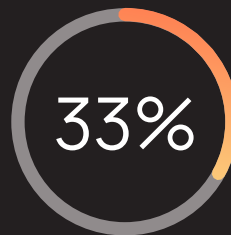
33% Would recommend a career in IT

**33%** Would discourage a career in IT

The strain on CFOs

As we know, CFOs control the overall budgets and shore up risks. It's clear that CFOs are under increasing pressure - 47% report feeling 'very' or 'extremely' stressed, compared to only 28% of IT Directors/Managers and 37% of IT security specialists. They are also more likely to have seen their level of stress increase in the past 12 months (71% compared with only 60% of IT leaders and 56% of IT security specialists). CFOs are more than twice as likely as their colleagues in IT security to consider an increase in cybersecurity incidents as a stress in their day-to-day work.

With IT risks increasing and cybersecurity teams ever more critical for the success or failure of organizations, a renewed focus on collaboration is needed to ensure teams are aligned and feel valued and engaged. CFOs and cybersecurity teams need to work together to understand how day-to-day work could be supported and improved.
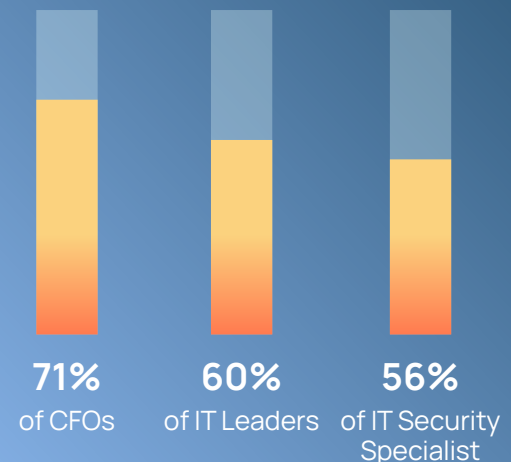
High employee turnover and stressed professionals negatively impact an organization's short–and long–term performance. And the growing volume and sophistication of cyber threats make it more critical than ever for organizations to manage workloads and give teams the support they need. There are several ways to achieve this – starting with regular check-ins with staff to understand their workloads, evaluate skills gaps, and other areas for development, create formal feedback mechanisms (like suggestion boxes or an email address), and even rewarding feedback.

Whether it's an investment in additional employees and training, a more relaxed working environment (such as more opportunities to work from home), or even equipping staff with transformative security tools like ThreatConnect, those that follow through on these improvements will be able to attract the best talent and keep their workforce happy and productive.

Creating an attractive workplace for professionals is key to protecting a business's long-term security. And this won't just make the lives of the IT staff more manageable, but those of the C-suite, too. After all, the more investment that CFOs make into their SecOps teams, the less likely their business will be harmed by cyber attacks—and the fewer on-the-job stressors they'll face.

37%
IT security specialists

47%
CFOs

28%
IT Directors / Managers
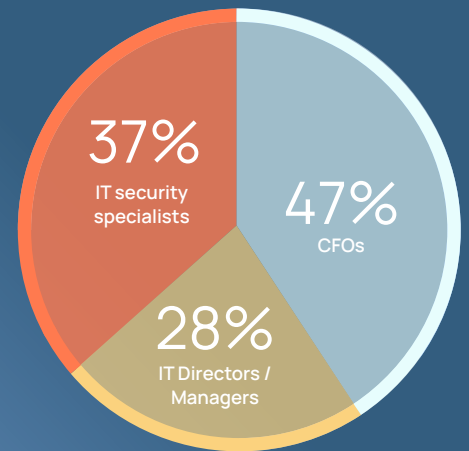
Stress Levels Increased In The Last 12 Months

71%
of CFOs

60%
of IT Leaders

56%
of IT Security Specialist

03

What More Can Be Done To
'Fix' Cybersecurity?

SecOps teams operate in a world full of systemic risk fueled by forces beyond their control. This includes the heightened risk of cyber attacks compounded by significant recruitment and retention issues, making organizations more vulnerable to potential attacks. Now, more than ever, security teams are expected to do more with less, leading to increased stress and threat risk levels.

Security teams need to translate cyber risk into terms that business executives can understand, bridging the gap between cybersecurity and business. By having security and business working from the same page, risk mitigation becomes the main priority – protecting the organization from harm. Security leadership will know which risks matter most; threat teams will know where to focus their attention.

By bringing risk quantification, threat intelligence, and security orchestration automation, and response together, teams can achieve a result that is essential to the future of security: organizations understand what financial risks current real-world cyber threats pose and provide them with a unified, efficient, and streamlined means of responding to the risks that are most important to their business.

At ThreatConnect, the Risk-Threat-Response Paradigm is the union between Cyber Risk Quantification (CRQ), a Threat Intelligence Platform (TIP), and a Security Orchestration and Automation (SOAR) Platform. We believe the first step in tackling core business challenges starts with understanding the strategic advantages of shifting to a risk-led, intelligence-driven security program.

Reduce complexity for business leaders and security operations teams alike.

Make decision-making easy by turning intelligence into action.

Continually reduce risk and strengthen defenses – within a set of internal feedback loops that work toward continuous improvement.

Unify processes and technologies.

The ThreatConnect Platform, built on an industry-leading threat intelligence platform, enables security teams to confidently forge their path to smarter security with intel-powered security operations.

ThreatConnect enables the operationalization of cyber threat intelligence analysis and management, and by leveraging native automation, orchestration, and knowledge capture, it lets teams work smarter, faster, and better – together. ThreatConnect provides Smarter Security to Help Security Teams Win – Every. Single. Day.

Contact us to learn more about how ThreatConnect can help you realize Intelligence-Powered Security Operations.

+1 (800) 965.2708   -or-   **ThreatConnect.com/Request-a-Demo**

ThreatConnect.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203
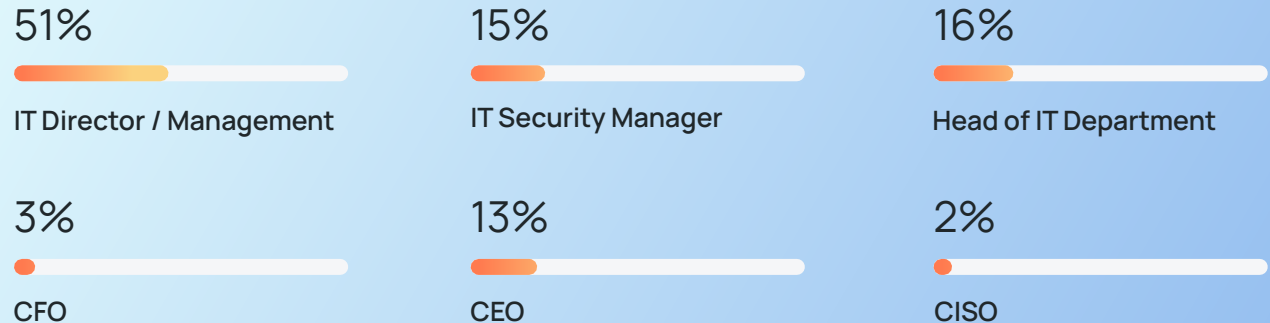
sales@threatconnect.com

+1 (800) 965.2708

04
Methodology

The ThreatConnect IT Under Stress report is based on a survey of 503 senior managers across the UK and US, responsible for making technology or IT Security decisions for their organizations. Sapio Research conducted online interviews on behalf of ThreatConnect in October 2021.

Country of Residence

UK
200 responses

40%

US
303 responses

60%

Job Role

51%

IT Director / Management

15%

IT Security Manager

16%

Head of IT Department

3%

CFO

13%

CEO

2%

CISO

Level of Responsibility for Cybersecurity

21%

Cybersecurity is a small part of my role

22%

Cybersecurity is a large part of my role but I have no decision-making authority

57%

Cybersecurity is a large part of my role, and I have decision-making authority