

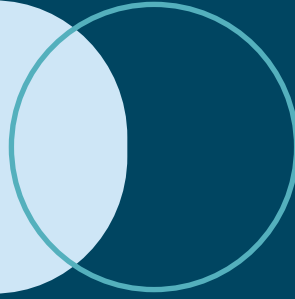
RESEARCH CONDUCTED BY



IN PARTNERSHIP WITH



MultiTeam
SOLUTIONS



RESEARCH REPORT • CYBERSECURITY PROFESSIONALS IN THE NETHERLANDS

Retaining Cybersecurity Talent: A Leadership Opportunity

Turnover in cybersecurity, at its current scale and scope,
is not inevitable.

This report is being published by
the Municipality of The Hague,
in partnership with MultiTeam Solutions

Initial Release
October 2026

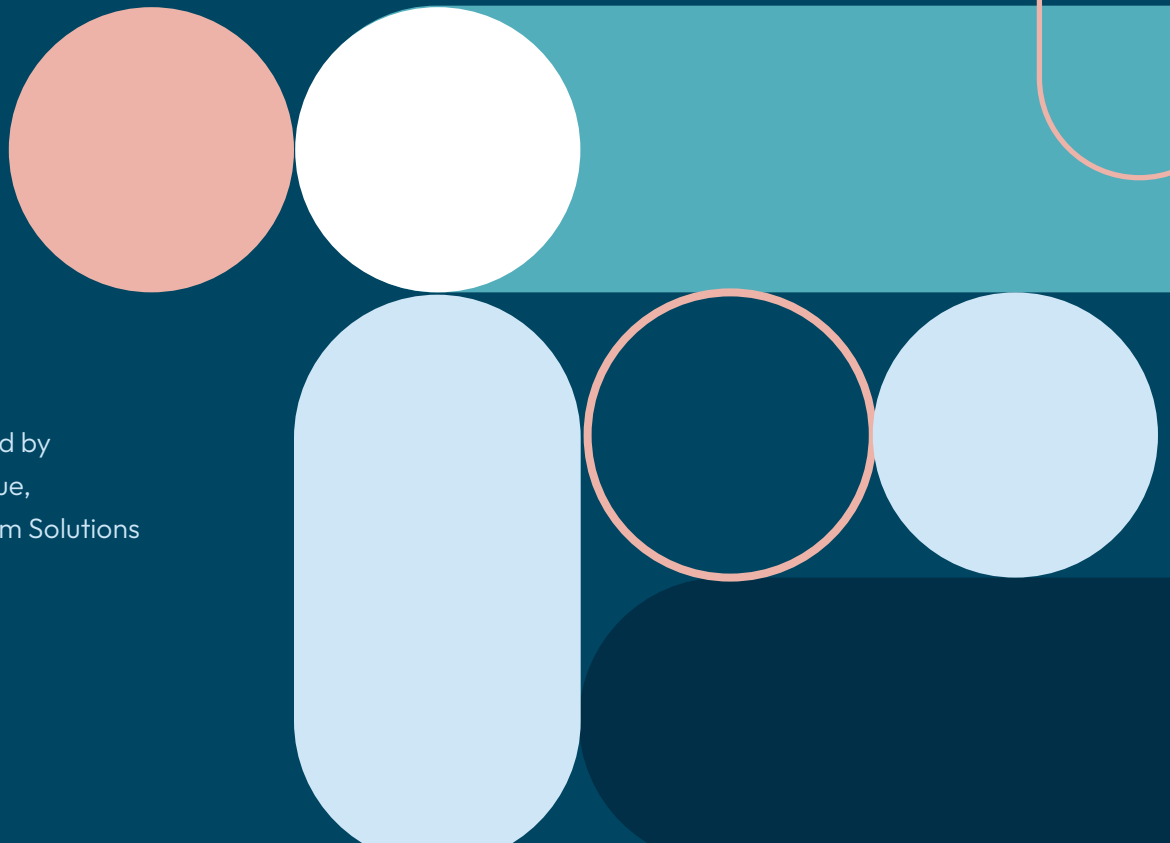


Table of Contents

A LETTER FROM THE RESEARCHERS	3
EXECUTIVE SUMMARY	5
WHY THIS IS URGENT	6
CONCEPTS & FRAMEWORK	7
METHODOLOGY, PARTICIPANTS & TRANSPARENCY	9
KEY FINDINGS	13
IN THEIR WORDS	17
THE SURROUNDING CONDITION	19
IMPLICATIONS	20
THE PRACTICAL PATH	21
CALL TO ACTION	24
LIMITATIONS	25
FUTURE RESEARCH	26



A Letter From The Researchers

Cybersecurity teamwork, individuals, and the environment around them:

Our journey with the Dutch security community began in 2012, through government-funded research supported by the Dutch NCSC in partnership with U.S. and Swedish government counterparts. The mandate was to better understand the human factors that drive effective teamwork in cybersecurity.

We have been fortunate to continue that journey with the Dutch security community — including work with public, private, and non-profit organisations, and sharing our work at the ONE Conference over multiple years — and now through this partnership with the Municipality of The Hague. The original question about teamwork has stayed with us, though our lens has widened over time.

The wider lens

Over the years, through research and applying the research in organisations, we have increasingly come to understand that effective teamwork cannot be separated from the individuals on each team and the environment in which people are being asked to work. That environment shapes how people think, collaborate, make decisions, handle pressure, and, ultimately, whether they are able to and choose to remain in their jobs. And that, in turn, has increasingly focused our attention on the role of leaders in shaping those conditions.

The water we swim in

There are two fish swimming along and they happen to meet another fish swimming the other way, who nods at them and says, “Good morning! How’s the water?” and keeps on swimming. The two fish swim on for a bit, and then eventually one of them looks over at the other and goes “What the hell is water?”

PARABLE BY DAVID FOSTER WALLACE (SLIGHTLY ADAPTED)

Cybersecurity has its own water: Constant urgency, incomplete information, competing priorities, work that is never quite finished, pressure that rarely disappears long enough for people to fully recover. Over time, these conditions — and the stress, burnout, and turnover that can accompany them — can start to feel simply like the way cybersecurity is.

Our research starts from a different premise: when something becomes the water we swim, the first challenge is seeing the water.

What helps people keep going

One foundation for understanding what helps people operate within demanding environments is the ABCs of motivation :

- **Autonomy** — having meaningful ownership and choice
- **Belonging** — feeling connected to and valued by others
- **Competence** — feeling capable of doing the work well, and seeing evidence of that capability

Together, these conditions help sustain motivation and individual resilience under pressure. And individual resilience matters beyond the individual: it contributes to the capacity of teams, organisations, and ultimately the wider cybersecurity community to continue operating effectively through challenge and change.

Why we did this research

This study represents another step in that journey. Together with the Municipality of The Hague, we wanted to better understand the working conditions experienced by cybersecurity professionals in the Netherlands — and, importantly, where leaders and organisations have meaningful opportunities to influence them.

The findings that follow reinforce something we have come to believe more strongly over nearly fifteen years of this work:

“Pressure may be inherent to cybersecurity. Its consequences do not have to be.”

By making the human side of the work more visible, we can begin to measure it, understand it, and act on it. We hope this report helps do exactly that.

Sincerely,

Daniel & Zac

MultiTeam Solutions

EXECUTIVE SUMMARY

The levels of stress, burnout, and turnover in cybersecurity are real.

They are also more within your control than it may seem.

Across cybersecurity, constant, elevated pressure and the resulting stress, burnout, and turnover have all quietly become the water that cybersecurity professionals swim in, accepted as the inevitable costs of working in the industry. These conditions, however, are changeable and, in turn, certainly do not need to be as extreme as they are currently being experienced. When a skilled cybersecurity professional reaches the point of leaving their job, their institutional knowledge, expertise, trust, and rapport all leave with them, which also disrupts operational stability and continuity — and in a field built on camaraderie, one departure can pull others toward the door.

This report is about the part of the talent gap that often gets less attention though may present a significant opportunity: keeping the skilled people who are already in the room.

Recruitment, reskilling, and upskilling all widen the talent pipeline, though each approach can take months, if not years, to generate benefits. Retention works the other side of the equation, and it is an approach where leaders have opportunities to act now.

Focused on cybersecurity in the Netherlands, this study by the Municipality of The Hague examined the relationships between 1) a focused set of human factors and leadership-related factors and 2) the outcomes of stress, burnout, and intentions to leave one's current organisation. In doing so, the study was designed to increase visibility on a specific group of conditions that leaders and organisations can influence, rather than compare these factors against a more comprehensive range of other reasons people may leave, such as compensation, career progression, or personal circumstances. What was found should be read as both a high-priority alert and as an invitation: important conditions associated with stress, burnout, and intentions to leave are currently invisible and unmeasured — and the data from this study increases visibility on where leaders and organisations may have opportunities to intervene.

KEY FINDINGS

Two protective factors stand out.

Supervisor support and a person's sense of competence — one's belief that they are doing their job well — were shown to each independently reduce stress, burnout, and one's intention to leave their job.

Competence can be protective on two fronts.

A supervisor who strengthens their own sense of competence protects themselves from stress, burnout, and feeling like they want to, or need to, leave. By being a more competent supervisor who better supports those they supervise, they can strengthen the competence of those people too, with the same protective outcomes.

Expressing stress improves one's disposition.

The findings suggest that one's ability to express stress to colleagues and supervisors in the workplace is related to perceptions of trust and reduced burnout.

The internal challenges add to the external challenges.

In addition to the everyday challenges presented by external adversaries, participants spoke about the pressure and stress created by the environment and leaders in their organisations.

WHAT TO DO ABOUT IT

The human layer of cyber risk is real and measurable, and the challenges associated with it are ones leaders can act on — often with more certainty of impact than acting on any aspect of the operational threat landscape.

1

Make it visible

2

Measure it

3

Manage it

While there is no feasible way to eliminate pressure, stress, burnout, or one's likelihood to leave, there are ways to take control and reduce these challenges at the individual and organisational levels.

01 · WHY THIS IS URGENT

Human factors are an unmeasured layer of cyber risk.

Organisations meticulously measure their technology and their threats. Far fewer measure the pressure, stress, and support levels of the people running the defence — even though those shape decision quality, coordination, and who stays.

What goes unmeasured cannot be managed, and right now the human layer is mostly invisible.

The overlooked front in the talent gap

Recruitment, reskilling, and upskilling each can take months if not years to yield results. While these approaches widen the pipeline of talent, retention works the other side of the equation — it slows the loss of the talent you already have — and it is an approach that leaders can act on now with relatively immediate benefits.

Retention is always going to be influenced by a multitude of factors, and this study focused specifically on human and leadership-related factors. Pay, benefits, holidays, promotions, and other possible drivers were outside the scope of this study. The cybersecurity professionals we spoke with emphasised elements of work that leaders control more directly: how they are managed, supported, and led.

When a skilled cybersecurity professional reaches the point of leaving their job, their institutional knowledge, expertise, trust, and rapport all leave with them, which also disrupts operational stability and continuity — and in a field built on camaraderie, one departure can pull others toward the door. Considering that seats are often hard to fill due to a limited talent pool and the subsequently competitive market for the talent that is available, there are only so many remedies available.

The opportunity to develop leaders

Focus group participants described a familiar challenge: technically capable professionals can move into leadership without equivalent preparation for the people-oriented side, or human factors, of the role. Deep technical skill and the skill of supporting people are different capabilities, and participants described leadership development as sporadic and under-resourced. That is an addressable gap.

This study in context

Retention is a recognised challenge within the wider cybersecurity workforce, and existing research helps place the focus of this study in context. For example, a Dutch study by Dialogic and Platform Talent voor Technologie that was commissioned to examine education and the cybersecurity labour market, identified both growing demand for cybersecurity expertise and a broader challenge around attracting and retaining current cybersecurity professionals. Its analysis also showed substantial movement within and beyond the organisations included in its research sample, while cautioning that moving outside those organisations did not necessarily mean leaving cybersecurity as a profession.

International research by IANS and Artico Search similarly reinforces the talent retention challenge in cybersecurity and emphasises that it is multi-factorial. In their 2026 survey of 515 cybersecurity professionals, only 34% reported intending to stay with their current employer, while job satisfaction was associated with career progression, compensation, and work-life balance. The report calls for a multi-pronged approach to satisfaction and retention — including wage growth, flexible work arrangements, and investment in a strong security culture in which people feel valued — further illustrating that retention extends beyond any single intervention or condition and includes people feeling valued.

This current study by The Municipality of the Hague adds a more focused lens to this wider picture by examining human factors and leadership-related factors that may offer leaders and organisations additional opportunities to support talent retention.

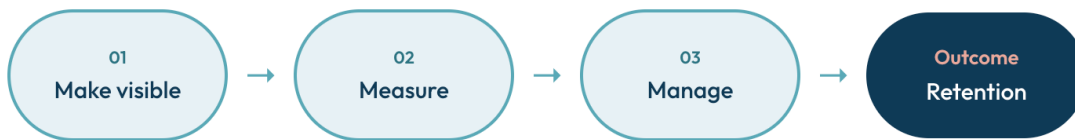
REFERENCES

- Dialogic & Platform Talent voor Technologie (PTvT), Onderwijs en Arbeidsmarkt Cybersecurity: Onderzoeksrapportage (2024). Commissioned by the Dutch Ministry of Economic Affairs and Climate Policy.
- IANS Research & Artico Search, 2026 Cybersecurity Talent Report (2026).

02 · CONCEPTS & FRAMEWORK

Make the invisible visible — then measure it, then manage it.

The research was built to surface what cybersecurity organisations have stopped seeing: the impact of constant, elevated pressure and the opportunities to reduce the stress, burnout, and turnover that have become accepted as part of the everyday, inevitable conditions in cybersecurity. You cannot, however, manage what you cannot see.



While it's not feasible to eliminate pressure, it is feasible to gain visibility on the impact of that pressure, measure it, and then manage it intentionally.

Against this backdrop, two protective factors were shown by this research to be consistently related to outcomes of lower stress, burnout, and turnover intention:

- 1) a person's sense of competence — one's belief that they are doing their job well — and
- 2) feeling supported by one's direct supervisor. Other motivational factors, including autonomy (a sense of ownership and control) and belonging (a sense of identity and community), also were shown to help reduce some of the outcomes measured.

03 · METHODOLOGY, PARTICIPANTS & TRANSPARENCY

Who we heard from, and how:

The Municipality of The Hague commissioned this study to better understand — and act on — the retention of the region’s cybersecurity professionals. It builds on fifteen years of social-behavioural cybersecurity research contributed by the municipality’s research partner, MultiTeam Solutions, with the Dutch security community involved from the outset. There were two sources of data for the study, which was conducted from mid-2025 to early 2026: a quantitative survey of 86 professionals, which carries the statistical findings, and three focus groups, conducted in English, and designed to illuminate and give context to the findings.

The statistical analyses and findings of this study reflect the human factors and leadership-related factors experienced by the cybersecurity professionals who participated in the research. The strength of the findings suggests that they may also generalise to cybersecurity professionals across the Netherlands.

Who was surveyed		
RESPONDENTS 86 cybersecurity professionals	FIELDWORK Mid-2025 to early 2026	AGE 35–64 for most respondents, evenly distributed
ROLES Operational · individual contributors · management	FUNCTIONS Governance, risk & compliance · policy · security consulting	ORGANISATIONS Public & private · mostly 250–999 staff, some 10k+

The 86 respondents were relatively evenly distributed across age groups. They were experienced in cybersecurity and, notably, well-represented in leadership: roughly four in ten sat at management level or above. The sample was almost evenly split between the public and private sectors, and was primarily from organisations with under 1,000 employees. Participants represented a wide variety of functions, and skewed primarily toward identifying as male. **See the following page for a detailed breakdown of the demographics of survey respondents**

The qualitative data draws from 6 optional open-ended survey questions and three hour-long focus groups. The focus group questions were devised from the survey findings, so the sessions were guided rather than entirely open-ended and designed to deepen and probe what the survey data had surfaced. All focus group data was anonymised.

Age

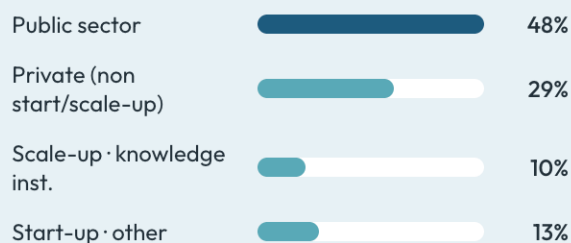
n = 86

**Role level**

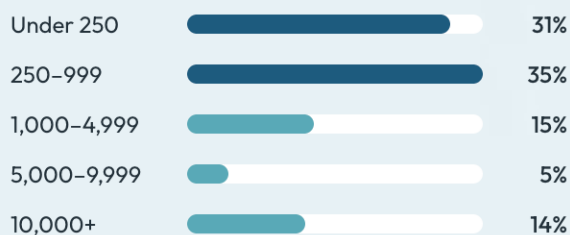
n = 86

**Organisation type**

n = 86

**Organisation size**

n = 86

**Primary function**

Respondents could select more than one

**78%**

aged 35–64

~41%

at management level or above

83 / 16 / 1%

male · female · non-binary

Analytical approach

Quantitative relationships were examined through correlation and regression analyses, including moderation analyses. Qualitative responses were analysed thematically. Dutch responses were translated to English and back-translated to Dutch for accuracy.

A NOTE ON MEASUREMENT, STATED PLAINLY

Turnover Intention was measured reliably and anchors the headline findings, though it is important to note that intention is a proxy for future behaviour and does not establish that respondents actually left. Burnout was measured with a four-item scale and showed low reliability, meaning the items were less consistent with one another as indicators of a single underlying construct; lower reliability tends to weaken observed relationships, so statistically significant associations may actually be understated; nevertheless, findings involving burnout should be interpreted more cautiously; also, the burnout measure reflects self-reported experiences rather than a clinical diagnosis.

What we measured — the three outcome scales

Each outcome was measured with a short multi-item scale. For transparency, the items are listed below; the protective-factor scales (supervisor support and competence) appear later, in the findings. Note that Turnover Intention in this study refers to intention to leave one's current organisation, not intention to leave cybersecurity as a profession.

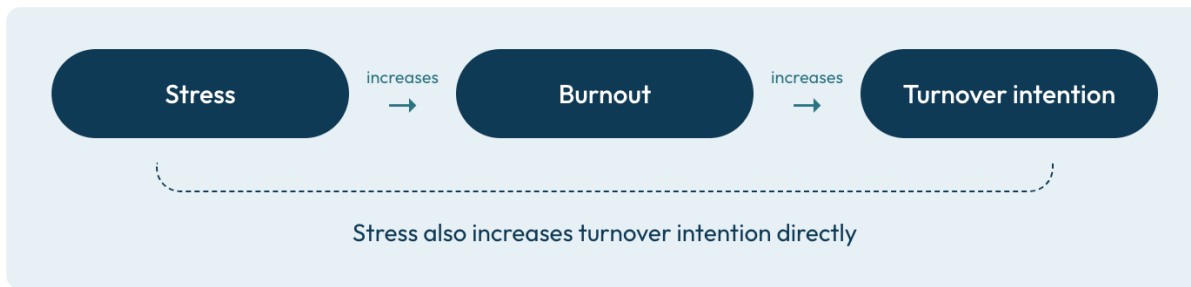
Stress	5 ITEMS	Burnout	4 ITEMS	Turnover intention	3 ITEMS
I am able to handle the amount of work I am assigned. ^R		I am proud of the work I do. ^R		I am satisfied with the job I currently have. ^R	
The pace of my work is manageable. ^R		I get discouraged when I feel like my work isn't going well.		I often consider if I should go work for a different organisation.	
My work increases my stress.		I have the motivation I need to do my job well. ^R		I plan to leave my current job in the next... ^R	
I am satisfied with my work-life balance. ^R		My work is emotionally exhausting.		0–5 months · 6–12 months · 1–2 years · 3–5 years · no current plan to leave	
I am able to quickly recover from stressful work events. ^R					

^R Reverse-coded — worded in the opposite direction and scored inversely, so that across each scale a higher score consistently indicates more of the outcome (more stress, more burnout, greater intent to leave).

04 · KEY FINDINGS

How stress, burnout, and turnover relate:

The three outcomes are not independent. In the regression models, stress significantly predicted both higher burnout and higher turnover intention, and burnout in turn predicted higher turnover intention.



Each relationship was positive and significant: stress increases burnout and turnover intention; burnout increases turnover intention.

A. Two protective factors

The findings suggested there were two factors that, as they increased, consistently decreased (i.e., protected against) stress, burnout, and intentions to leave one's job: a person's sense of competence and the support of their direct supervisor.

PROTECTIVE FACTOR — RELATIONAL

Supervisor support

Four elements assessed together:

- 1) I have support from my direct supervisor to do my job well;
- 2) I do not feel like my direct supervisor understands what's important to me;
- 3) My direct supervisor acknowledges my contributions;
- 4) I am able to express when I'm feeling stressed to my direct supervisor.

PROTECTIVE FACTOR — INDIVIDUAL

Sense of competence

Three elements assessed together:

- 1) I am good at the work I do;
- 2) I receive clear feedback about the quality of my work;
- 3) I know what I am expected to do in my job.

NOTE: The study was not longitudinal, so the causal relationships are inferred from statistical models testing the effects of supervisor support and competence on the outcomes.



The two protective factors — each associated with lower stress, burnout, and likelihood to leave.

Expressing your stress can build resilience

Another opportunity to change one's disposition that the data pointed to was the protective factor of being able to express your stress. Two complementary elements of stress expression were assessed together:

SURVEY ITEM 1

"I am able to express when I'm feeling stressed to colleagues."

SURVEY ITEM 2

"I am able to express when I'm feeling stressed to my direct supervisor."

At work, and in cybersecurity in particular, there are many reasons people may suppress their stress rather than express it — pressure, shame, acceptance of the stressful conditions they work in, etc. When held long enough, stress will tend to surface anyway. In this study, expressing stress and trust each predicted the other, so the two clearly are related — though which causes which is unclear, and the relationship may well be cyclical, with each increasing the other over time. Expressing stress was also associated with lower burnout (a correlation, not a causal effect). The wider point is the one that matters for leaders: there are additional levers to pull beyond building competence and supervisors providing support. This serves as yet another opportunity to first make the invisible visible and then create an environment that turns that visibility into action and change.

The open-ended questions on the survey and experiences shared by the focus group participants echoed the protective factors. Guided by the initial findings of the survey, the sessions probed and deepened the findings and validated the importance of the relationship with direct supervisors and one's sense of competence.



Most of my stress comes from managers who keep changing priorities midway, always have “emergencies,” and don’t agree with how I’ve prioritised.”

— SURVEY RESPONDENT · “WHAT CAUSES YOU STRESS?”

“Meeste stress komt door leidinggevendens die tussentijds taken van prioriteit veranderen, altijd (zogenoemd) spoedjes hebben...” · translated & back-translated from Dutch



It’s not a technical problem. It’s a social problem — it’s about not being able to work together. And if you’re only fighting inside, when are you supposed to fight outside?”

— FOCUS-GROUP PARTICIPANT · AGGREGATED & ANONYMISED

One participant described bringing a worked-through problem to their manager for a second perspective, and hearing only the question turned back on them:



Asking for help is already a barrier I have to get through — and I was explicitly asking, and not getting it. It seemed unfair that I wanted to leave my position over one person.”

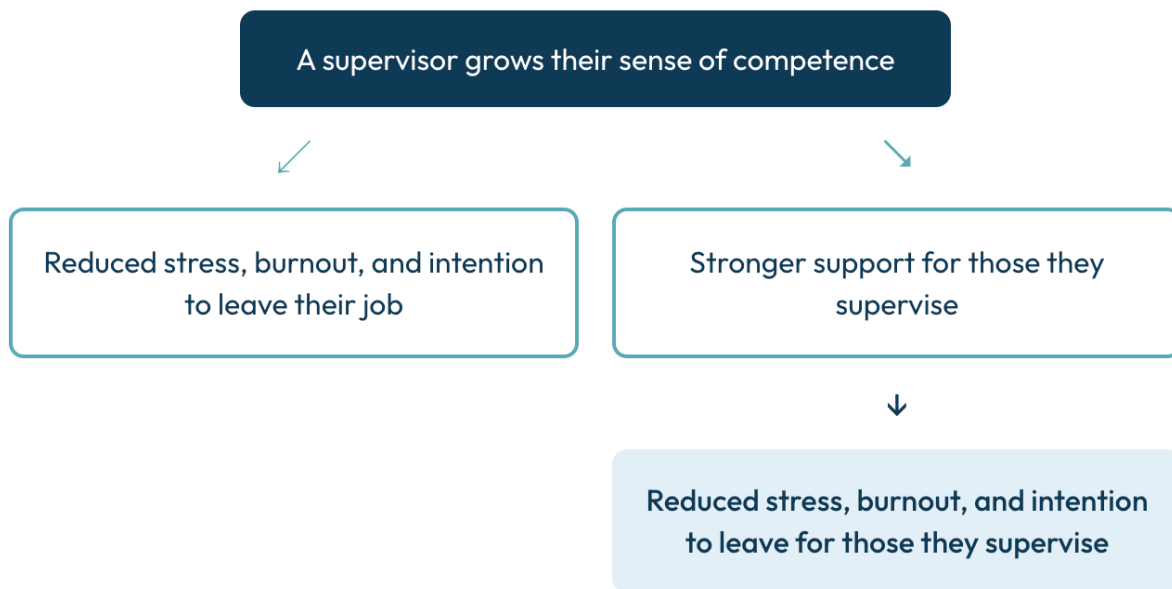
— FOCUS-GROUP PARTICIPANT · AGGREGATED & ANONYMISED

This statement, in particular, illustrates one plausible pathway to losing talent: an unsupportive supervisory relationship contributing to an otherwise committed professional considering leaving. It is also, encouragingly, the exact kind of condition that leaders can learn to change.

04 · KEY FINDINGS, CONTINUED

B. The competence multiplier

The findings suggest that competence is a protective factor, and developing competence for supervisors can allow the same effort to pay off twice. When a supervisor builds their own competence it can simultaneously allow them to better support and build competence for those they supervise, having a multiplicative effect.



A supervisor who grows their competence could build their own resilience while also strengthening the resilience of those they supervise.

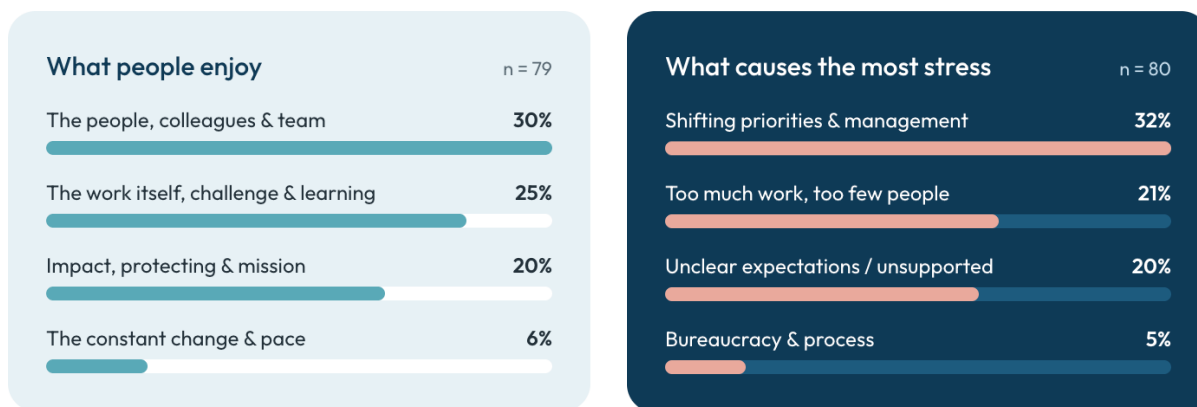
For the supervisor, competence can include gaining control over how pressure impacts them, communicating more effectively, acknowledging progress and successes, and more. For those they supervise, competence can show up as better supervisory support and a stronger sense of their own competence. One lever, pulled once, moves two needles — which points to why investing in leadership development is a high-leverage opportunity.

05 · IN THEIR WORDS

The numbers illuminated by the voices:

Coding the open-ended survey responses surfaces a consistent picture. Asked what causes the most stress, the largest share pointed not at the threat outside but at the environment inside the organisation. Asked what they enjoy, the answers ran the other way — toward the people, the work itself, and the sense of protecting something that matters.

Placed side by side, the two lists indicate that people value the mission and each other; what wears them down is the environment around the work.



Thematic coding of open-ended responses. Many responses touched more than one theme, so percentages do not sum to 100%; figures are approximate and indicate relative frequency.

People came into cybersecurity because of the type of work — and the environment — and they continue to enjoy a wide range of aspects, from the challenge of the work to the pace to the sense of protecting something that matters.



The field is always moving, and the feeling that you genuinely contribute something.”

— “WHAT DO YOU ENJOY?”

“het vakgebied is zo in beweging en het gevoel hebben dat je daadwerkelijk iets bijdraagt...” · translated & back-translated from Dutch

What can wear people down is not having the opportunities and capacity to do the work well, including too much work being carried by too few.



It stresses me when I carry too many responsibilities and tasks while there are too few experienced colleagues to share the work with.”

— “WHAT CAUSES YOU STRESS?”

“Het geeft me veel stress als ik te veel verantwoordelijkheden en taken heb, terwijl er te weinig ervaren collega's zijn...” · translated & back-translated from Dutch

And when asked what support would help, people pointed to leadership competencies such as listening and regular feedback.



Check in and give feedback more regularly.”

— “WHAT COULD YOUR SUPERVISOR OR COLLEAGUES DO TO SUPPORT YOU?”

“regelmatiger peilen en feedback geven” · translated & back-translated from Dutch

From the focus groups

On the quiet grind of work that is never finished:



I've had to redefine what “enough” means — to be less than what it could be.”

— FOCUS-GROUP PARTICIPANT · AGGREGATED & ANONYMIZED

On why a sense of competence is so hard to hold onto in this field — because success is measured in things that don't happen:



“The absence of something bad is not the same as the presence of something good.”

— FOCUS-GROUP PARTICIPANT · AGGREGATED & ANONYMIZED

And on what can keep people:



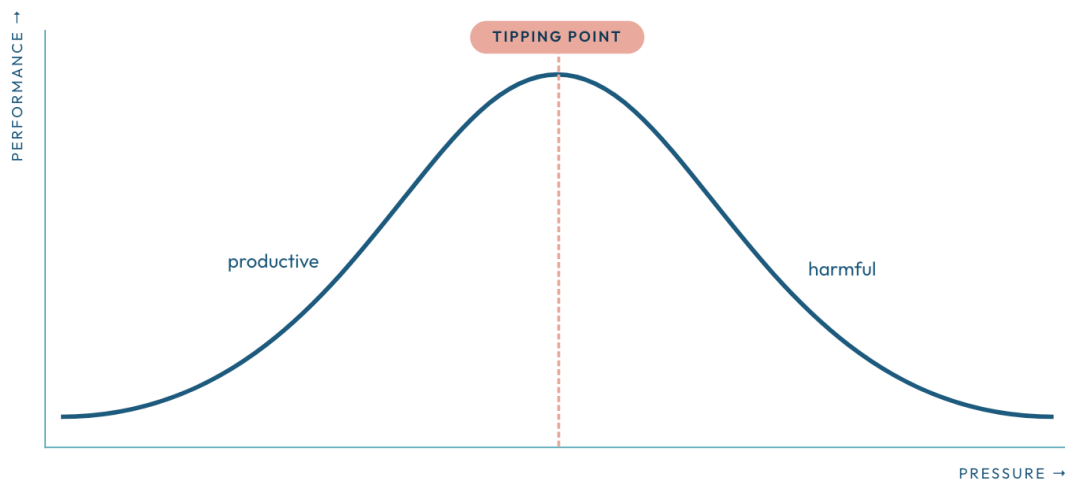
“The work culture is so good, it keeps us here. I travel a long way every day, and I do it happily.”

— FOCUS-GROUP PARTICIPANT · AGGREGATED & ANONYMIZED

06 · THE SURROUNDING CONDITION

Pressure is an inherent part of the environment.

In cybersecurity, pressure is a ubiquitous condition surrounding the work — and its effect depends, in part, on how much is experienced by each individual. In line with the Yerkes-Dodson model, pressure can have benefits to one’s work. Sustained and/or extremely high levels of pressure, especially without room to recover, can push past a person’s tipping point.



A tipping-point relationship: pressure helps up to a point, then turns costly — the goal is to manage where you sit on the curve.



The work is “never finished.” “There’s always so much to do,” and, plainly, “it makes me feel tired.” And the pressure rarely starts with the leader: “my manager is also under a lot of pressure from senior management,” and it “trickles down to everybody.””

— FOCUS-GROUP PARTICIPANTS · AGGREGATED & ANONYMIZED

Leaders sit in the middle of that chain — which is also where they can interrupt it.

07 · IMPLICATIONS

What this all means — for leaders and for organisations:

While this study only explores a few components of a wider retention picture, the evidence suggests there are reasons talented professionals may consider leaving that involve behaviours and perceptions leaders can influence more than they may realise. These are opportunities for leverage. The challenges are ones that, with support, one can see, measure, and act on.

For cybersecurity leaders

- Build your own competence; it is the buffer that also allows you to better support your people
- Give positive and constructive feedback deliberately, even when pressure pushes you to delay or ignore it
- Acknowledge progress out loud — it is one way to strengthen how competent you and your people feel
- Treat pressure as something to see and manage, not just endure, because you cannot manage what stays invisible

For organisations

- Recognise what turnover includes: knowledge and trust walking out the door, decision bottlenecks for those who are left, and the possible contagion of one departure prompting others
- Measure the human layer alongside the technical one, because it is a genuine input to operational risk
- Invest in leaders developing leadership skills, because technical skills are not leadership skills
- View leadership training and development as contributing to your retention infrastructure

08 · THE PRACTICAL PATH

Leadership training around three skills:

The findings point most clearly toward three teachable leadership skills — each one strengthening the competence and support that contribute to employee retention. They are the basis of leadership training opportunities the Municipality of The Hague is now bringing to cybersecurity professionals in the Netherlands.

WHAT THIS TRAINING WILL INCLUDE

A new initiative designed to increase visibility on challenges and conditions while serving as an inflection point (as opposed to a destination) in developing cybersecurity leadership. The focus groups made a case for this type of leadership training: leaders described the training they get today as sporadic and under-resourced — “whatever falls from the sky,” in one participant’s words — with organisations assuming leadership “will just happen.” One significant gap, then, is a training that is designed to take into account both the technical experts who become leaders in cybersecurity and the high-pressure, high-stakes cybersecurity environment in which they lead.

LEADERSHIP SKILL

Gaining visibility on pressure

WHY THE SKILL?

Pressure is constantly felt yet rarely examined. Cybersecurity leaders constantly experience pressure that, often, they have never named, quantified, or parsed into what they can and cannot influence.

WHY IT MATTERS FOR RETENTION

You cannot manage what you cannot see. Naming pressure is an important step toward protecting your own resilience.

WHERE TO START

Identify up to three sources of regular to constant pressure on you. Rate each for intensity, frequency, and how much control you have — then create a plan to address the sources of pressure that have the greatest impact on you and that you also have the most control over.

LEADERSHIP SKILL

Giving feedback to those you supervise

WHY THE SKILL?

Under pressure, it can be easy to deprioritise feedback and never quite get to it. In turn, feedback is often delayed, softened, or skipped. Developmental feedback (future-oriented coaching) does more for retention than evaluative feedback alone.

WHY IT MATTERS FOR RETENTION

Developmental feedback is a key way that competence is built in others — and respondents named it directly. As one focus-group participant put it, “I’m very feedback-driven — if I’m just doing things and not getting feedback, I start to question myself.”

WHERE TO START

Identify an opportunity to give forward-thinking, supportive feedback around a single behaviour or moment (e.g. a decision-making outcome, communication, collaboration) with the goal of improving the recipient’s skills. Key criteria for the feedback include being genuine, specific, and timely.

LEADERSHIP SKILL

Acknowledging progress & successes

WHY THE SKILL?

In cybersecurity, success is often measured in things that don't happen — a truth one focus-group participant captured: "the absence of something bad is not the same as the presence of something good." Then consider this condition under constant pressure, where there is almost always a next thing to focus on, so progress and wins can easily go unrecognised.

WHY IT MATTERS FOR RETENTION

Recognising progress is one way people perceive their own competence and believe their effort is making a difference.

WHERE TO START

Walk back through a recent project. Find where something moved forward, a good call was made, or things went better than expected — acknowledge key moments or signs of progress and success. Also notice which of those moments were never acknowledged out loud.

FOR MORE INFORMATION

Learn about upcoming cybersecurity leadership training events through the Municipality of The Hague by visiting the website through the URL or QR code below

<https://thehague.com/cybersecurity/en/one-day-leadership-training-leading-under-pressure>



09 · CALL TO ACTION

Make it visible. Measure it. Manage it.

Make it visible

Surface the human layer of cyber risk — starting with educating cyber professionals in order to raise awareness about 1) the various sources of pressure that impact them, 2) default behaviours and mindsets, and 3) what they can do to help build individual resilience for themselves and those they lead.

Measure it

Gather and track metrics around perceptions of competence and supervisory support, stress and burnout levels, and intent to leave alongside the technical metrics already watched so closely.

Manage it

Equip leaders via leadership development initiatives to grow their competencies around navigating pressure, giving feedback, and acknowledging progress and successes so they can better support themselves and those they lead.

Levels of stress, burnout, and turnover intention are not fixed. This study identifies several conditions that impact these levels and that both leaders and organisations can influence while recognising that retention is also going to be shaped by factors beyond the scope of this research.

The professionals we heard from generally and greatly value the mission they serve and the work they do. Giving them support and reasons to stay in their organisations can and should become a higher priority.

Limitations of this Research

A strength of this study is its deliberate focus on cybersecurity professionals in the Netherlands. The research was designed to surface cybersecurity-specific human factors and leadership-related factors within this high-pressure, high-stakes professional environment. The study, relying on cross-sectional, self-report data from a general sample of cybersecurity professionals, was sufficient to identify meaningful, statistically significant relationships, though not to definitively identify causality over time or take into account current turnover levels across specific organisations.

Two measurement considerations are also important. Turnover Intention was measured as intention to leave one's current organisation, rather than whether someone ultimately changed employers or left cybersecurity altogether. The Burnout measure also showed low reliability, so findings involving Burnout should be interpreted with additional caution.

The sample may also underrepresent several perspectives. Everyone surveyed was a current cybersecurity professional, meaning those who had already left the field or were on extended leave because of burnout may be less represented. The sample was also predominantly male (83%), limiting the diversity of perspectives represented.

Future research

Future research could build on this study in a variety of ways:

- Larger and more diverse samples as well as longitudinal data collection (i.e., across multiple time points)
- Longitudinal research to strengthen the testing of causal relationships between supervisor support and competence and the outcomes of stress, burnout, and turnover intention, while also making it possible to examine how these relationships change over time
- A more deliberate effort to hear from cybersecurity professionals who identify as female or non-binary as well as those who have left cybersecurity or experienced burnout-related leave
- Compare organisations with higher and lower turnover, distinguish between movement between employers and exits from cybersecurity, and strengthen the measurement tool used for burnout
- Examine whether improved leadership and working conditions primarily influence how cybersecurity talent moves between organisations or whether they reduce overall exits from cybersecurity, which would help clarify the extent to which stronger leadership practices function as an organisational advantage versus a cybersecurity-wide retention mechanism in attracting and retaining talent.

The findings raise a practical, explicit hypothesis for future studies: to what extent does a supervisor strengthening their own competence allow them to better support and build competence in those they supervise. If confirmed longitudinally, the argument to invest in this type of focused leadership development would be strengthened even further.

Ultimately, this study makes it clear that there is 1) an immediate opportunity and highly likely benefit to building leadership skills and abilities for cybersecurity leaders that support both the leaders themselves and those they lead and 2) longer-term opportunities to measure the impact of such leadership development and further explore this topic through future research.

Contact Dr. Daniel Shore at MultiTeam Solutions for more information regarding this study or any other questions or comments regarding the topics addressed.

Daniel@MultiTeam.solutions

You can also learn more about MultiTeam Solutions and their approach to leadership training for cybersecurity professionals at <https://MultiTeam.solutions>