

# HUMAN CAPITAL IN CYBERSECURITY – HOW TO STOP WASTING IT

PROF. M. ANGELA SASSE FRENG, ML  
PROFESSOR OF HUMAN-CENTRED SECURITY  
RUHR-UNIVERSITÄT BOCHUM

# CASA ExZELLENZCLUSTER BOCHUM



# OVERVIEW

1. Human Capital in organisations
2. How we (mise)use it in cyber security
3. Impact on different groups of cybersecurity experts and employees
4. The way forward: honesty, cooperation, baby steps, leadership engagement

# HUMAN CAPITAL

- Similar concept first described by Adam Smith (1776): Investment made in education and training of individuals in a society is a resource in itself, more important than capital and natural resources. [1]
- *Human Capital Theory* by Becker (1964): Tangible assets are not the only forms of capital. Education, medical care, and moral values are examples of capital, because they increase gains, income, and improve health and therefore their costs should be considered as an investment in human capital. [2]

[1] Eide, E. R., & Showalter, M. H. (2010). *Human capital*. DJ Brewer and P. McEwan (section eds), *International Encyclopedia of Education, Economics of Education Section*.

[2] Kwon, D. B. (2009, October). *Human capital and its measurement*. In *The 3rd OECD world forum on “statistics, knowledge and policy” charting progress, building visions, improving life* (pp. 27-30).

# HUMAN CAPITAL AND ORGANIZATIONS

- Positive relation between human capital and:
  - Employee performance [1]
  - Organizational effectiveness [2]
  - Firm's growth rate [3]



[1] Saeedi, N., Alipour, A., Mirzapour, S. A., & Chaboki, M. M. (2012). Ranking the intellectual capital components using fuzzy TOPSIS technique (case study: an Iranian company). *Journal of basic and applied scientific research*, 2(10), 10360-10368.

[2] Josan, I. J. (2013). Human capital and organizational effectiveness. *Manager*, (17), 39-45.

[3]. Channar, Z. A., Talreja, S., & Bai, M. (2015). Impact of human capital variables on the effectiveness of the organizations. *Pakistan Journal of Commerce and Social Sciences (PJCSS)*, 9(1), 228-240.



# HUMAN CAPITAL AND WELL-BEING

- Individuals will bring their knowledge, skills, abilities and other characteristics to an organization, but such contributions are intertwined by their health and well-being. [1]
- Well-being: Physical, psychological and emotional health, comfort and happiness of employees. [2]
- Workers who experience high levels of well-being also perform well and vice versa. [3]



[1] Nielsen, K., Nielsen, M. B., Ogbonnaya, C., Käsälä, M., Saari, E., & Isaksson, K. (2017). Workplace resources to improve both employee well-being and performance: A systematic review and meta-analysis. *Work & stress*, 31(2), 101-120.

[2] Pradhan, R. K., & Hati, L. (2022). The measurement of employee well-being: development and validation of a scale. *Global Business Review*, 23(2), 385-407.

[3] Wright, T. A., & Cropanzano, R. (2000). Psychological well-being and job satisfaction as predictors of job performance. *Journal of occupational health psychology*, 5(1), 84.

# HUMAN CAPITAL IN SECURITY

- Cybersecurity: complex work field with many different professions
- ENISA: 12 role profiles for cybersecurity professionals [1]
- Plus: Employees

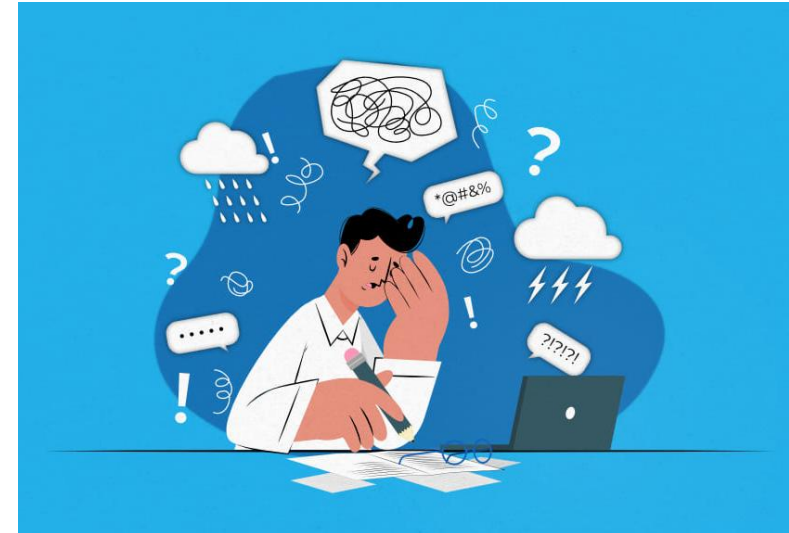


[1] European Union Agency for Cybersecurity (ENISA), "European Cybersecurity Skills Framework (ECSF) - User Manual," ENISA, Tech. Rep., September 2022

# KEY PROBLEM: STRESS

## 2. Decline in job performance [1], [2]:

- Decreased organizational performance
- Decreased employees' overall performance
- Decreased quality of labour
- High staff turnover
- Absenteeism



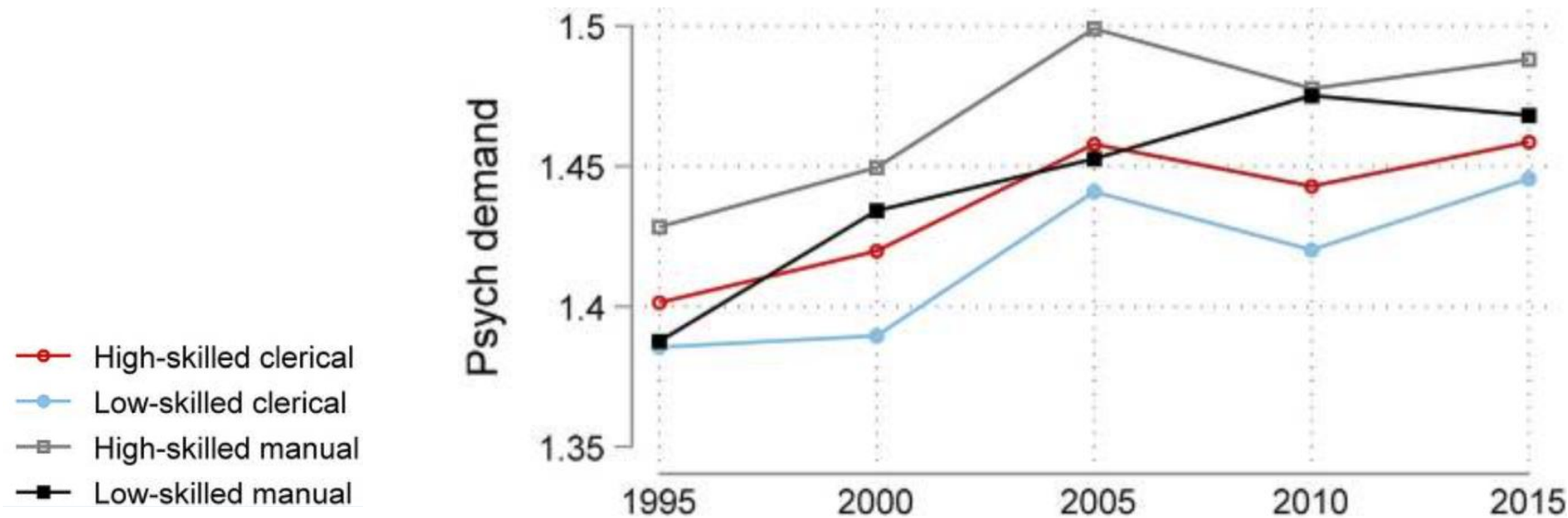
[1] Yu, J., Park, J., & Hyun, S. S. (2021). Impacts of the COVID-19 pandemic on employees' work stress, well-being, mental health, organizational citizenship behavior, and employee-customer identification. *Journal of Hospitality Marketing & Management*, 30(5), 529-548.

[2] Pandey, D. L. (2020). Work stress and employee performance: an assessment of impact of work stress. *International Research Journal of Human Resource and Social Sciences*, 7(05), 124-135.



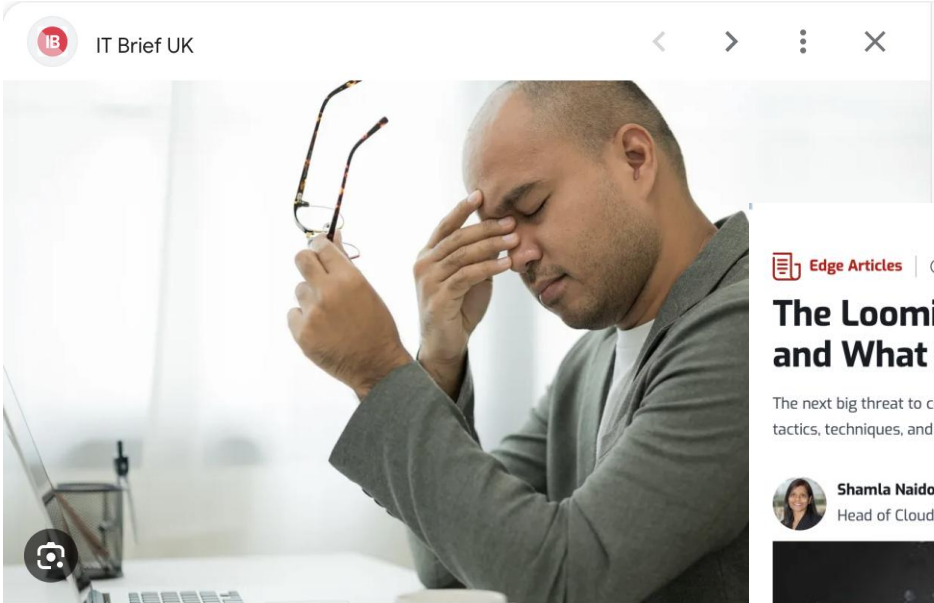
# STRESS LEVELS HAVE BEEN RISING

- Work stress generally increased from 1995 to 2015, and that the increase was mostly driven by psychological demands[1]



[1] Rigó, M., Dragano, N., Wahrendorf, M., Siegrist, J., & Lunau, T. (2021). Work stress on rise? Comparative analysis of trends in work stressors using the European working conditions survey. *International Archives of Occupational and Environmental Health*, 94, 459-474.

# CISOS AND STRESS



The rise of CISO stress: Recognising and reconciling the threat of litigation for CISOs

**Edge Articles** | 4 MIN READ | THE EDGE

## The Looming CISO Mental Health Crisis — and What to Do About It, Part 1

The next big threat to corporate security may not be a new strain of malware or innovative attacker tactics, techniques, and processes. It may be our own mental health.

**Shamla Naidoo**  
Head of Cloud Strategy & Innovation, Netskope

January 28, 2022

A woman in a blue shirt is covering her face with her hands, looking distressed. The word "Stress" is overlaid in large orange letters. The background is dark with some text and graphics.

**SC Media**  
A CRA Resource

CISO STORIES TOPICS EVENTS PODCASTS RESEARCH RECOGNITION LEA

Security Staff Acquisition & Development, Leadership, Data Security

**CISO stress levels are out of control**

Daniel Klein June 21, 2023

A man in a suit is covering his face with his hands, looking distressed. The background is a blurred office environment.

# CISOS AND STRESS

Nominet Cyber Security Survey (2019) [1]:

- Survey of 408 CISOs.
- Most are dealing with a cybersecurity talent shortage which adversely contributes to human performance, often in the form of stress, burnout, and fatigue.
- 17% of CISOs used medication or alcohol to cope with stress.
- 60% of CISOs rarely unplug from their jobs.
- 88% reported working more than 40 hours per week.



[1] Nominet Cyber Security. (2019). *Life inside the perimeter: Understanding the modern CISO*. Retrieved from [Nominet-Cyber\\_CISO-report\\_FINAL-130219.pdf](#).

# CISOS AND STRESS

- The continuous stress and mental health implications disrupt the CISOs work-life balance; 88% of the executive were overly stressed. [1]
- CISOs are responsible for a myriad of responsibilities, leading to too much strain and stress. The nature of the CISO position results in short tenures from 1 to 2 years due to the increasing responsibility, less personal and recovery time, and the constant connectivity. [2]



[1] Sheridan, K. 90% of CISOs would pay for better work-life balance. DarkReading.com. Retrieved from <https://www.darkreading.com/risk/90--of-cisos-wouldcut-pay-for-better-work-life-balance/d/d-id/1336995>

[2] ISACA. (2020, November 18). *Understanding and burning CISO burnout*. ISACA.org.

# CISOS AND FRICTION

## **Lacking the Tools and Support to Fix Friction: Results from an Interview Study with Security Managers**

Jonas Hielscher, Markus Schöps, Uta Menges, Marco Gutfleisch,  
Mirko Helbling, and M. Angela Sasse, *Ruhr University Bochum*

Compliance-driven approach and demand for metrics from leadership

*“That leaves ISO27001 again. Because it is the most established. [...] The goal is: ‘I want this certification.’ And, to put it bluntly, you’re almost walking over dead bodies. So now you [the employees] have to do it like this.”*

[1] Hielscher, J., Schöps, M., Menges, U., Gutfleisch, M., Helbling, M., & Sasse, M. A. (2023). Lacking the tools and support to fix friction: results from an interview study with security managers. In Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023) (pp. 131-150).



# INHERENT ROLE PROBLEMS

*“Cyber security is analogous to a belief system and how one of the roles of the CISO is akin to that of a modern-day soothsayer for senior management; that this role is precarious and, at the same time, superior, leading to alienation within the organisation.” [1]*

*Masculine and militaristic self image, norms, and practices. Projecting strength is exhausting.*

*Especially keeping it up in the face of everyday experience of failure.*



[1] Da Silva, J. (2022). Cyber security and the Leviathan. Computers & Security, 116, 102674.

# EMPLOYEES AND ITS: STRESS

- Relation between high email load, stress and susceptibility to phishing emails. [1]
- Relation between high work-load and the likelihood of employees clicking on a phishing link. [2]
- Low level of job stress associated with higher levels of information security awareness [3]



[1] Rozentals, E. (2021). *Email load and stress impact on susceptibility to phishing and scam emails.*

[2] Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). *Why employees (still) click on phishing links: investigation in hospitals.* *Journal of medical Internet research*, 22(1), e16775.

[3] McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., & Lillie, M. (2018). *The effect of resilience and job stress on information security awareness.* *Information & Computer Security*, 26(3), 277-289.

# EMPLOYEES AND SECURITY-RELATED STRESS

- **Security-Related Stress (SRS):** Stressful demands imposed by security requirements. [1]
- Security requirements can backfire and provoke noncompliance due to the stressful demands they impose upon employees. [2]
- SRS showed negative correlations with Perceived Occupational Stress, Perception of IT Department Communication, and Employee Trust in IT Department. [3]

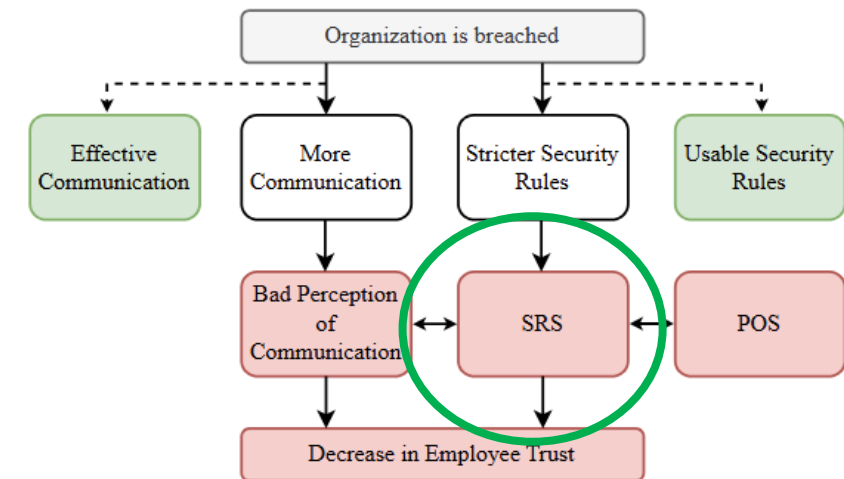


Fig. 2. Diagram showing relevant results and recommendations discussed in sections V-B, V-C and V-D. SRS = Security-Related Stress; POS = Perceived Occupational Stress; Green = positive outcome; Red = negative outcome.

[1] D'Arcy, J., & Teh, P. L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, 56(7), 103151.

[2] D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 29(1), 43-69.

[3] Schöps, M, Shanthakumar, S, Müntefer, P, & Sasse, M.A. "Even after two years, we still have a bad feeling": Two Comparative Case Studies of the Effects of a Cyberattack on Fear, Trust in the IT Department and Security-Related Stress. Unpublished

# EMPLOYEES AND ITS: PHISHING

**Simulated Stress:  
A Case Study of the Effects of a Simulated Phishing Campaign on Employees'  
Perception, Stress and Self-Efficacy**

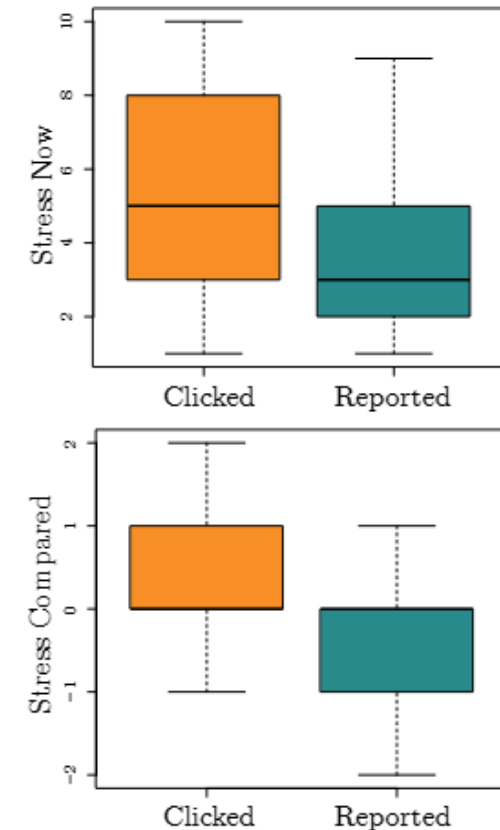
Markus Schöps  
Ruhr University Bochum, Germany

Marco Gutfleisch  
Ruhr University Bochum, Germany

Eric Wolter  
Ruhr University Bochum, Germany

M. Angela Sasse  
Ruhr University Bochum, Germany

- Employees who *clicked* reported significantly **more stress** (than before) and more stress than employees who *reported*. [1]
- Still: Most employees thought that simulated phishing campaigns were effective, and many that stress was necessary (**teachable moment**).



[1]. Schöps, M., Gutfleisch, M., Wolter, E., & Sasse, M. A. (2024). Simulated Stress: A Case Study of the Effects of a Simulated Phishing Campaign on Employees' Perception, Stress and {Self-Efficacy}. In 33rd USENIX Security Symposium (USENIX Security 24) (pp. 4589-4606).

# EMPLOYEES AND ITS: LEARNING

- Stress before or during learning can block the retrieval of memories. [1]
- Stress before learning improves memory formation. [2]  
**But:** Only for emotionally arousing, especially negative, memory elements, and at the cost of neutral elements. [3]
- Stress during learning: Formation of both neutral and emotional memory is impaired. [4]



[1]. Schwabe, L., Hermans, E. J., Joëls, M., & Roozendaal, B. (2022). Mechanisms of memory under stress. *Neuron*, 110(9), 1450-1467.

[2] Henckens, M. J., Hermans, E. J., Pu, Z., Joëls, M., & Fernández, G. (2009). Stressed memories: how acute stress affects memory formation in humans. *Journal of Neuroscience*, 29(32), 10111-10119.

[3] Wolf, O. T. (2009). Stress and memory in humans: twelve years of progress?. *Brain research*, 1293, 142-154.

[4] Schwabe, L., & Wolf, O. T. (2010). Learning under stress impairs memory formation. *Neurobiology of learning and memory*, 93(2), 183-188.



# EMPLOYEES AND ITS: PHISHING CAMPAIGNS

- Simulated Phishing Campaigns: One of the most propagated countermeasures and a billion-dollar market.
- Measure employees' ability to recognize phishing emails and to sensitize and train employees.
- Embedded training as part of SPCs is not effective. [1]

## Phishing in Organizations: Findings from a Large-Scale and Long-Term Study

Daniele Lain, Kari Kostiainen, and Srdjan Čapkun  
Department of Computer Science  
ETH Zurich, Switzerland  
{daniele.lain, kari.kostiainen, srdjan.capkun} @inf.ethz.ch

The experiment ran for 15 months with more than 14,000 study participants (employees of the company).

Embedded training during simulated phishing exercises does not make employees more resilient to phishing, but instead it can have unexpected side effects that can make employees even more susceptible to phishing: false sense of security. [1]

[1]. Lain, D., Kostiainen, K., & Čapkun, S. (2022, May). *Phishing in organizations: Findings from a large-scale and long-term study*. In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 842-859). IEEE.

# EMPLOYEES AND ITS: MANUFACTURING WORKERS

## Noise and Stress Don't Help With Learning: A Qualitative Study to Inform Design of Effective Cybersecurity Awareness in Manufacturing Environments

- 33 manufacturing workers in 6 locations, to determine what they knew about cybersecurity risks, to what extent they consider them relevant, and what their experiences with, and perceptions of cybersecurity measures and training were. [1]
- Results:
  - Not enough of staff at work = high workload and time pressure
  - IT systems not working smoothly or being too slow
  - Cybersecurity friction at work
    - High number of emails and messages with irrelevant information.
    - Friction with authentication
    - Training via kiosks on noisy shop floor

[1] Brunken, M. Schöps, A. Buckmann, F. Meißner, M. A. Sasse. Noise and Stress Don't Help With Learning: A Qualitative Study to Inform Design of Effective Cybersecurity Awareness in Manufacturing Environments. TBP ACM-CCS 2025

# ITS STAFF: SRS

**”Even after two years, we still have a bad feeling”:  
Two Comparative Case Studies of the Effects of a Cyberattack on Fear, Trust in the IT  
Department and Security-Related Stress.**

- Security-Related Stress (SRS) is also present for ITS staff. [1]
- From Interviews with IT department: IT security requirements often led to friction for employees.
- Also: participants stated that the security requirements led to friction for themselves, negatively influencing productivity. Mentioning documentation requirements, long passwords, updates, multiple accounts, screen time outs, and complex authentication methods as reasons.






*“Through documentation requirements and also through the security that we have introduced with multiple accounts and so on. This creates more work and also means that you have to do more work around your work, which ultimately costs time.”*

*„Schöps, M, Shanthakumar, S, Müntefer, P, & Sasse, M.A. ”Even after two years, we still have a bad feeling”: Two Comparative Case Studies of the Effects of a Cyberattack on Fear, Trust in the IT Department and Security-Related Stress. Procs. EuroUSEC 2025.*

# EMPLOYEES AND ITS EXPERTS

- Security relationships are often dysfunctional. [1]
- Among security consulting companies, blaming employees is common.
- Several sources of conflict in participants' relationship with ITS staff:
  - *Frequent misunderstandings and obstacles in communication due to a lack of shared language.*
  - *Differing expectations of ITS staff's tasks and lack of knowledge of employees' work requirements.*
- Also: Negativity in communication and feelings, power imbalance, emotional disengagement, blaming.


## Why IT Security Needs Therapy

Uta Menges<sup>1</sup>(✉) , Jonas Hielscher<sup>2</sup> , Annalina Buckmann<sup>2</sup> ,  
Annette Kluge<sup>1</sup> , M. Angela Sasse<sup>2</sup> , and Imogen Verret<sup>2</sup>

[1] Menges, U., Hielscher, J., Buckmann, A., Kluge, A., Sasse, M. A., & Verret, I. (2021, October). Why it security needs therapy. In European Symposium on Research in Computer Security (pp. 335-356). Cham: Springer International Publishing..

# SECURITY CHAMPIONS

## Security Champions Without Support: Results from a Case Study with OWASP SAMM in a Large-Scale E-Commerce Enterprise

Authors:  [Marco Gutfleisch](#),  [Markus Schöps](#),  [Stefan Albert Horstmann](#),  [Daniel Wichmann](#),  [M. Angela Sasse](#) | [Authors](#)  
[Info & Claims](#)

- secure software development practices
- security perception of different roles within the software teams
- Finding: security champions are given responsibility, but no tangible support



Software Assurance  
Maturity Model  
(SAMM)



Qualitative  
interviews

[1] M Gutfleisch, M Schöps, SA Horstmann, D Wichmann, MA Sasse: Security Champions Without Support: Results from a Case Study with OWASP SAMM in a Large E-Commerce Enterprise. EuroUSEC 2023



## Caring Not Scaring – An Evaluation of a Workshop to Train Apprentices as Security Champions

Uta Menges  
Jonas Hielscher  
Ruhr University Bochum  
Germany  
firstname.lastname@rub.de

Laura Kocksch  
Aalborg University Copenhagen  
Denmark  
firstname.lastname@ikl.aau.dk

Annette Kluge  
M. Angela Sasse  
Ruhr University Bochum  
Germany  
firstname.lastname@rub.de

### Corporate training workshop

- did not address apprentices' concerns or questions
- Material in part outdated/irrelevant/poor quality
- not adapted to organisations' technology and policies
- lots of scaring (them even more)
- attempts to self-organise a network (via WhatsApp) were squashed

[1] Menges, U., Hielscher, J., Kocksch, L., Kluge, A., & Sasse, M. A. (2023, October). Caring not scaring-an evaluation of a workshop to train apprentices as security champions. In *Proceedings of the 2023 European Symposium on Usable Security* (pp. 237-252).]

# SECURITY ANALYSTS

- Goal: Evaluate the mental health landscape of SOC practitioners using validated psychological scales.
- Alarmingly high levels of personal and work-related burnout among participants (approx. 31-36% of participants met the criteria for high burnout).
- Considerable deficiencies in mental and physical health, life satisfaction, and social connectedness compared to normative workplace benchmarks.

## Human Performance in Security Operations: A Survey on Burnout, Well-Being and Flow State Among Practitioners

Kashyap Thimmaraju  
Technische Universität Berlin & Flow Guard Institute  
kashyap.thimmaraju@tu-berlin.de

Sybe Izaak Rispens  
Independent Researcher  
sybe@rispens.de

Gail-Joon Ahn  
Arizona State University  
gahn@asu.edu

[1] Thimmaraju, K., Rispens, S. I., & Ahn, G. J. *Human Performance in Security Operations: A Survey on Burnout, Well-Being and Flow State Among Practitioners*.

# SECURITY ANALYSTS

- Security Operation Centers (SOCs) defend their enterprise networks in general and identify malicious behaviors in both networks and hosts.
- Anthropological study of a corporate SOC over a period of six months.
- Goal: Identify the factors that lead to analyst burnout and how it can be mitigated.

## A Human Capital Model for Mitigating Security Analyst Burnout

Sathya Chandran  
Sundaramurthy  
Kansas State University  
sathya@ksu.edu

Xinming Ou  
Kansas State University  
xou@ksu.edu

Alexandru G. Bardas  
Kansas State University  
bardasag@ksu.edu

Michael Wesch  
Kansas State University  
mwesch@ksu.edu

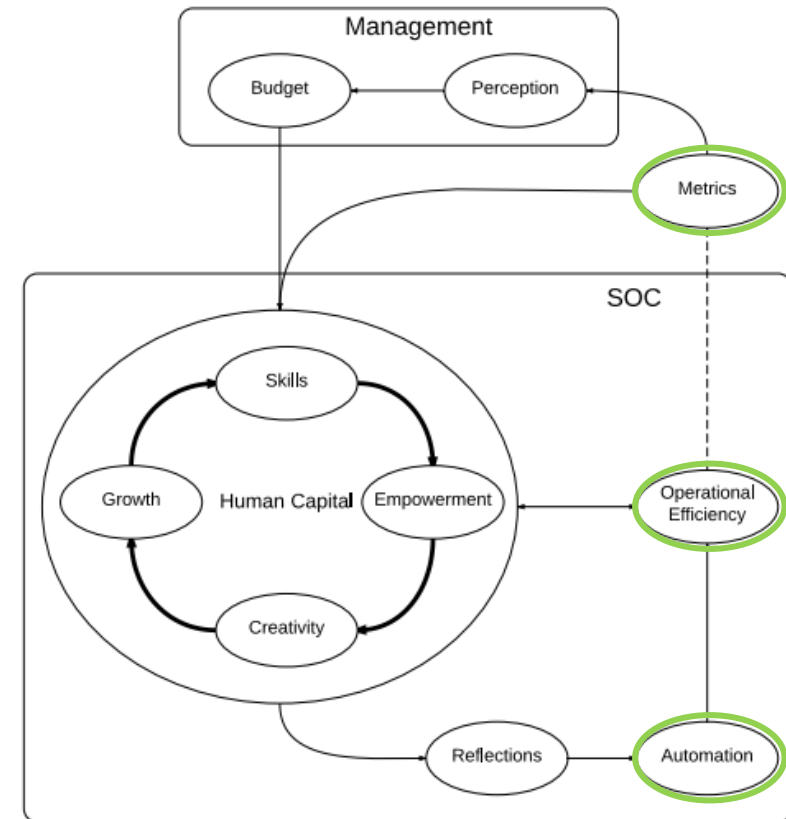
S. Raj Rajagopalan  
Honeywell ACS Labs  
siva.rajagopalan@honeywell.com

Jacob Case  
Kansas State University  
jacobcase94@ksu.edu

John McHugh  
RedJack, LLC  
john.mchugh@redjack.com

# SECURITY ANALYSTS

- Results: Burnout occurs due to a cyclic interaction of Human Capital with the following three categories:
  - Automation
  - Operational Efficiency
  - Management Metrics



[1] Sundaramurthy, S. C., Bardas, A. G., Case, J., Ou, X., Wesch, M., McHugh, J., & Rajagopalan, S. R. (2015). A human capital model for mitigating security analyst burnout. In *Eleventh symposium on usable privacy and security (SOUPS 2015)* (pp. 347-359).

# SECURITY ANALYSTS

- Automation: Software tools that aid analysts' job and improve operational efficiency.
- Results: Effective automation doesn't really take place.

*"At one point we had procedures written down for everything and analysts were starting to feel like robots performing the same tasks everyday. We did not have any reviews to refine the processes as at one point nobody was even documenting them properly."*

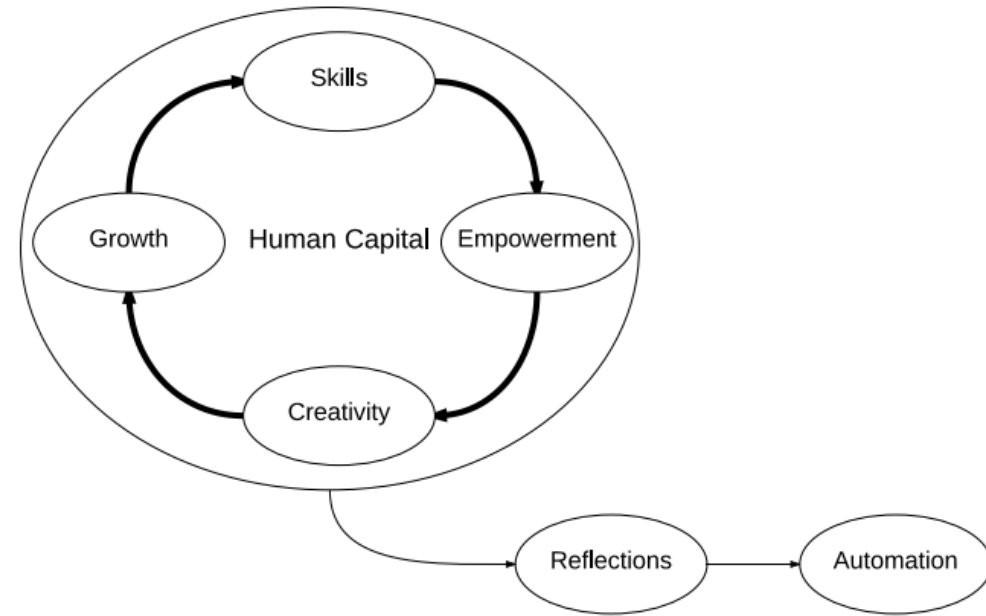


Figure 4: Automation



# SECURITY ANALYSTS

- Operational Efficiency: Leverage all resources of a SOC to detect and respond to threats in a timely manner.
- Highly skilled and creative analysts make operations efficient.
- Human Capital affects efficiency through automation: This accelerates operations—especially in case of highly repetitive tasks

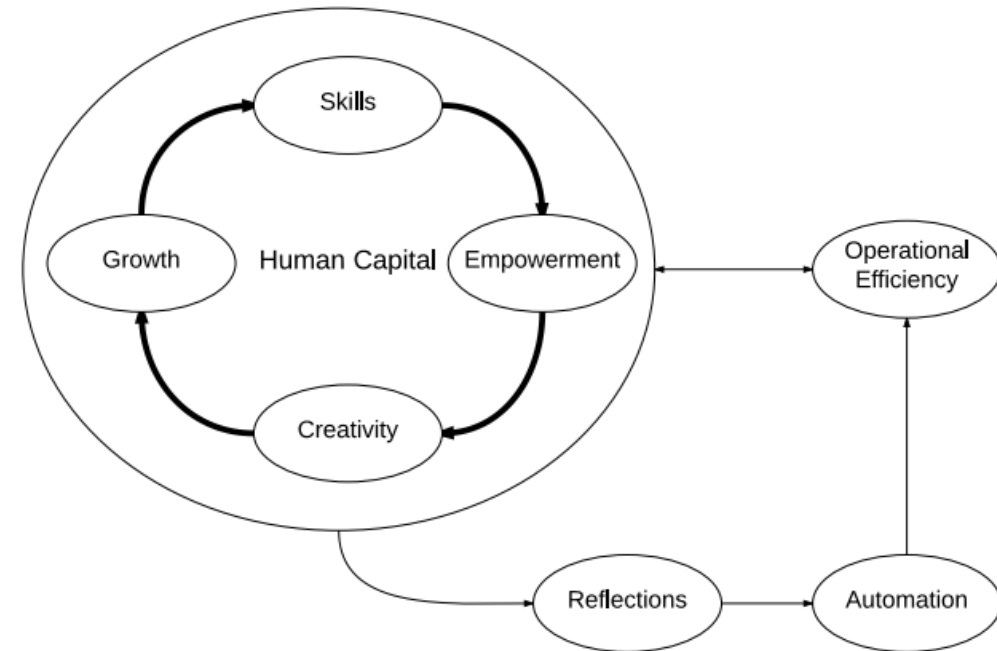


Figure 5: Operational Efficiency

# SECURITY ANALYSTS

- Management Metrics: Devising appropriate metrics is complicated by the fact that even the higher managers are not sure what shall be the right metrics.
- The pressure for good metrics is relayed down to the SOC managers who in turn hand it down to the analysts.

*“We feel that we are not doing security monitoring in the SOC. I think we are just working to generate numbers for higher management. We have raised some ethical concerns with the management regarding this.”*

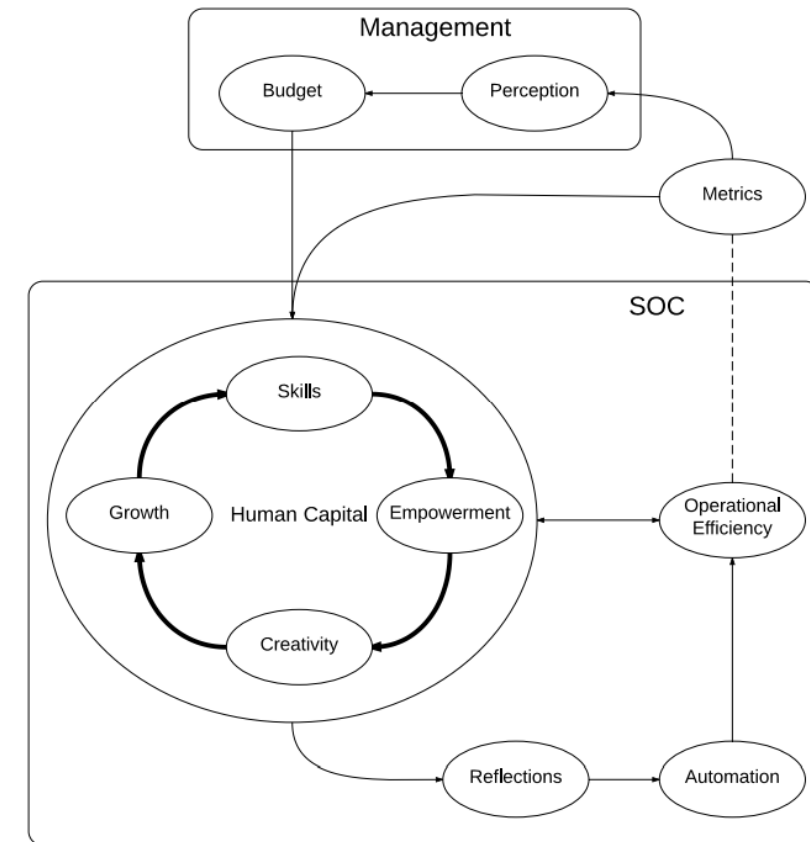


Figure 6: Metrics

[1] Sundaramurthy, S. C., Bardas, A. G., Case, J., Ou, X., Wesch, M., McHugh, J., & Rajagopalan, S. R. (2015). A human capital model for mitigating security analyst burnout. In Eleventh symposium on usable privacy and security (SOUPS 2015) (pp. 347-359).

# ROOT OF THE PROBLEMS

1. *Responsibilisation*
2. *Compliance Theatre and Fixation on (mostly useless) metrics*
3. *Security professionals' failure to evaluate, learn, improve (PDCA cycle)*
4. *Leadership failure to engage and invest*

# ROOT OF THE PROBLEM: RESPONSIBILISATION

*“cyber security is a policy area where the State continues to push responsibility away from itself and onto non-State actors, as a means of extending and enhancing the governance of situations and environments which have a tendency to produce criminal behaviour”*

National policies push responsibility onto small companies and their staff

- Who do not have capability and capacity to discharge it
- Government gets more frustrated with lack of progress
- Rule scepticism grows among staff in those companies

*Neil MacEwan: Responsibilisation, rules and rule-following concerning cyber security:  
Findings from Small Business Case Studies in the UK. PhD Thesis, University of Southampton 2017  
[https://eprints.soton.ac.uk/417156/1/Neil\\_MacEwan\\_Thesis\\_final\\_draft\\_post\\_viva\\_.pdf](https://eprints.soton.ac.uk/417156/1/Neil_MacEwan_Thesis_final_draft_post_viva_.pdf)*

# RESPONSIBILIZATION

- Neoliberalist approach = government does less protection
- individualizing risk: telling citizens and organisations how to protect themselves
- through directives, certifications (Cybersecurity Essentials, BSI Grundschutz, KRITIS Regulierung, now NIS-2)
- ... and then leaving them to face the consequences if they can't/won't follow advice

*K. Renaud, S. Flowerday, M. Warkentin, P. Cockshott. Is the responsabilization of the cyber security risk reasonable and judicious? Computers & Security, Volume 78, September 2018, Pages 198-211.*

# SECURITY THEATRE

Coined by Bruce Schneier, on TSA measures post-9/11

- National Guard deployed in US airports, without ammunition - good
- Ineffective bag scanning to lower insurance premium – also good

*“people who don’t understand security can be reassured with cosmetic or psychological measures, and sometimes that reassurance is important. It can be better understood by considering the many non-security purposes of a security system. A monitoring bracelet system that pairs new mothers and their babies may be security theater, considering the incredibly rare instances of baby snatching from hospitals. But it makes sense as a security system designed to alleviate fears of new mother.”*

<https://www.schneier.com/tag/security-theater/>



# “RATIONAL ASTROLOGIES”

Many measures today do not provide security, but serve another purpose for those who put them in place:

1. easier to follow the commonly used requirements, even when they make no sense, than to argue for more sensible one
2. to do something when faced with unsolvable problem
3. bureaucratic inertia: *“it’s always been done this way”*

*“Both security theater and rational astrologies may seem irrational, but they are rational from the perspective of the people making the decisions about security.”*

*J Kelsey, B Schneier : Rational Astrologies and Security. Festschrift Rossfest 2025*  
<https://www.cl.cam.ac.uk/events/rossfest/2025-stajano--rossfest-festschrift.pdf>

## COMPLIANCE MINDSET + “BEST PRACTICE”

- “Box-ticking”, as opposed to checking it has intended effect (which is why PDCA is so important)
- “*Just get it done*” – failure to engage or wanting to improve - one of the many bad outcomes of responsabilisation (MacEwan)
- Failure to engage with security issues, no interest in learning and improvement
- Waste of resources, manageable risks remain

# SUMMARY

Successful defence depends on human capital – stop wasting it

Security experts

- Invest in automation and better IT
- reduce stress and provide growth opportunities
- leadership engagement and support

Employees

- reduce security friction
- stop wasting time: targeted communication
- focus on behaviour not knowledge
- baby steps: “one secure routine at a time”

Support instead of responsabilisation

# ACCESSIBLE AND MEANINGFUL SUPPORT

The screenshot shows the homepage of Digital.Sicher.NRW. At the top left is the logo, which consists of a blue shield with a white grid pattern and the text "DIGITAL SICHER NRW" in yellow and white. To the right of the logo is a search bar with the placeholder text "Suchbegriff eingeben" and a magnifying glass icon. Below the logo and search bar is a horizontal navigation menu with the following items: "INFOMATERIAL", "DIGITALE ERSTBERATUNG", "NEWS", "NEWSLETTER", "VERANSTALTUNGEN", "JOBS", and "ÜBER UNS". To the right of the navigation menu is a yellow button with a shield icon and the text "SOFORTHILFE", followed by a white button with the text "HIER FINDEN!" and a right-pointing arrow. The main content area has a dark blue background with a subtle pattern of white lines. On the left side of the main content area is a white box with the text "Ihr Kompetenzzentrum für Cybersicherheit in der Wirtschaft." and a button below it that says "Unsere kostenlosen Angebote:" followed by a downward-pointing arrow. On the right side of the main content area is a section titled "DIGITAL.SICHER.NRW" with four icons and their corresponding labels: a clipboard icon for "Erstberatung", a piggy bank icon for "Fördermittel", a share icon for "Kontakt", and a megaphone icon for "Veranstaltungen".

**DIGITAL.SICHER.NRW**

Ihr Kompetenzzentrum für  
Cybersicherheit in der  
Wirtschaft.

Unsere kostenlosen Angebote: ▼

Erstberatung Fördermittel  
Kontakt Veranstaltungen

# CLEAN UP COMMUNICATION



KONTAKT

ENGLISH

 GEBÄRDENSPRACHE

 LEICHTE SPRACHE

Das BSI

Themen

IT-Sicherheitsvorfa

 > Service > Presse > Passwortwechseln war gestern: Wie Verbraucherinnen und Verbraucher ihre Benutzerkonten absichern können

Passwortwechseln war gestern: Wie  
Verbraucherinnen und Verbraucher  
ihre Benutzerkonten absichern  
können

**Ort** Bonn

**Datum** 31.01.2025