Teaching essential cognitive skills for resilient cybersecurity

Venkat Laxmi Sateesh Nutulapati

Objectives

- Highlight the need for cognitive skills training at early stages
- Map various cognitive skills to functional roles
- Present starting points for incorporating into curriculum

My background

- Technology
  - Director of Hosting & DevOps (NIST, FedRAMP, HIPAA, GDPR, etc)
  - Web app security for 200+ enterprise clients
- Dual master's in Psychology & Neuroscience
  - King's College London
  - University of Madras
- Human-centered cybersecurity
  - Full Member of Applied Neuroscience Association

Start with why

- The four components of the cyber world [18]

Singh 2024

Psychology in Cybersecurity: Unveiling the Human Dimensions of Digital Resilience

Start with why

- Let's expand "resilience"

Start with why

- Technological solutions are evolving; are the humans shielded too?
- Soft skills vs. cognitive skills (pilot choice)
- Industry expects training has taken care of the skills
- Training expects industry will build the skills on the job

Start with why

- Passion and motivation are expected to solve cognitive capability challenges – real world problems are boring
- Professionals cannot sell the services without using fear as the tool – what’s the mental health impact of this vigilance?
- If we do not operationalize, we cannot measure

Start with why

- Understanding resource-depletion versus self criticism.
- Can help with peak performance and avoid burnout
- Make wholesome future managers and leaders

The cost of a single lapse in judgement

MGM

2023[1]

10-min vishing of help-desk team

$100M hit

CAESARS

2023[2]

Social engineering of 3rd-party vendor

8-figure ransom

UBER

2022[3]

Bombarded with push notifications until approval

Internal code & vulnerabilities exposed

COLONIAL

2021[4]

Single leaked VPN password without MFA

$4.4 mil ransom (partially recovered)

Alarming stats

50% expect **burnout** within 12 months; 80% within 3 years.[5]

66% say cybersecurity is more **stressful** than 5 years ago.[6]

74% have taken mental-health **sick leave**; average 3.4 days/year lost.[7]

78% of SOC staff work 7+ hrs/week overtime; 71% may quit due to **alert fatigue.**[8]

83% say **burnout** led to **breach-causing errors**; 77% say stress harms data security.[9]

46% of orgs cite **work stress** as a key reason for **staff turnover.**[6]

Cognitive skills = Dual shields

- Cut breaches – Protect the business
- Boost people resilience – Improve performance

Starting point

- Feedback, revisions, adaptations are welcome

NICE Framework (SP 800-181) categories[11]*

Abbrev.	Category	What it covers (one-line summary)
SP	**Securely Provision**	Design, build and test secure IT/OT systems and software
OM	**Operate and Maintain**	Run, administer and sustain systems and data stores securely
OV	**Oversee and Govern**	Lead, manage, set policy, train and acquire for cybersecurity
PR	**Protect and Defend**	Detect, analyse and mitigate threats inside org networks
AN	**Analyze**	Produce cyber-intelligence from multi-source information
CO	**Collect and Operate**	Plan and execute offensive collection & cyber operations
IN	**Investigate**	Handle digital forensics and cyber-crime investigations

* Not Rev 1 - more practical to use Rev1 categories

Snapshot

Cognitive Domain	Impact Area	NICE Categories
Cognitive Flexibility	Dynamic environments, tool switching, escalation	OM, CO, SP
Bias Mitigation / Metacognition	Improved decision-making, intelligence analysis	AN, CO, SP, OV
Executive Control / Working Memory	Incident response, alert triage	PR, IN, OM
Situational Awareness/Emotional Intelligence	Performance under pressure, team cohesion	PR, IN, OV
Behavioral Pattern Recognition	Phishing, anomaly detection, malware behavior	AN, CO, PR
Psychological Ownership / Motivation	Policy adherence, secure development culture	OV, SP, OM
Stress management	Impacts all areas	All

Why early?

- Cognitive skills belong to the prefrontal cortex of the brain – fuel guzzler
- Neuroplasticity’s first inflection occurs at around 20 years of age

NICE Conference & Expo

Cognitive Flexibility

The ability to shift mental strategies quickly in response to new information or evolving situations.

Why it matters: Adversaries change tactics constantly and so do tools, threats, and business needs.[12]

Chowdhury et al., 2020

Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures

Bias Mitigation / Metacognition

The ability to notice your own assumptions and correct for bias in real time.

Why it matters: Cognitive shortcuts can lead to dangerous conclusions, especially under stress.[13]

Vishwanath et al., 2011
Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model

Executive Control / Working Memory

The ability to hold, prioritize, and process multiple inputs or tasks under pressure.

Why it matters: Cyber roles often require switching contexts rapidly from alerts to dashboards to incident notes while still staying precise.[14]

Diestel et al., 2013

Burnout and impaired cognitive functioning: The role of executive control in the performance of cognitive tasks

NICE Conference & Expo

Situational Awareness

The ability to perceive, understand, and anticipate what's happening in your environment both digitally and organizationally.

Why it matters: Security is dynamic. Being able to see the full picture helps you respond before issues escalate.[15]

Greenlee et al., 2016
Stress and Workload Profiles of Network Analysis: Not All Tasks Are Created Equal

Behavioral Pattern Recognition

The ability to detect deviations, anomalies, or repeated tactics in human or system behavior.

Why it matters: Many threats like phishing, lateral movement, insider attacks rely on subtle patterns.[13]

Vishwanath et al., 2011

Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model

Stress Management / Resilience

The ability to stay calm, recover quickly from setbacks, and keep a clear head in pressure situations.

Why it matters: Burnout, fatigue, and panic degrade performance especially in critical roles.[16]

Singh et al., 2023
Stress in the cybersecurity profession: A systematic review

Emotional Intelligence

Recognizing, understanding, and managing your own emotions and those of others.

Why it matters: Security is deeply human and how you collaborate, persuade, and de-escalate matters as much as your technical skill. [17]

Wiederhold, 2021
Increasing cybersecurity through emotional engagement

Psychological Ownership / Motivation

The feeling that "security is my responsibility," not just someone else's job.

Why it matters: Internal motivation creates stronger habits and more ethical decision-making. [18]

Menard et al., 2018

The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination

Action items for organizations

Start naming the cognitive skills in your team conversations.

- Example: When debriefing an incident, don’t just say “we missed it,” say “**we had a breakdown in situational awareness**” or “our **alert fatigue impacted** working memory.”
- This **language shift builds a culture** that recognizes and values thinking skills.

Map key roles in your organization to cognitive demands.

- Use the taxonomy we’ve discussed to identify high-pressure roles that require **training in attention, bias mitigation**, or resilience and build those into hiring, onboarding, and **professional development**.

Introduce micro-training on cognitive skills.

- 10-minute resilience exercises, daily bias checks, or pattern recognition challenges can be easily embedded into team routines.
- These skills compound over time **just like muscles**.

Bring learning and HR partners to the table.

- Elevate this conversation from "awareness training" to "**cognitive performance development**."
- Advocate for training investments that go beyond compliance and into capability.

Action items for academia

Integrate Cognitive Skills into Course Learning Outcomes

- Don’t treat cognitive skills as hidden curriculum.
- Explicitly include outcomes like:
  *“**Apply bias awareness** to threat analysis”* or
  “Demonstrate resilience in simulated incident response under time constraints.”
- This gives students **language to describe *how* they think**, not just *what* they do.

Use Scenario-Based Learning to Teach Metacognition and Bias Awareness

- Design labs or tabletop exercises where students **must challenge their own assumptions**.
- Example: Present ambiguous evidence in a forensics lab and require students to document how they ruled out red herrings.
- Turn **debriefing into a cognitive skills lesson**, not just a technical one.

Embed Micro-Reflections into Assignments and Labs

- Add one question at the end of each assignment:
  “What was your thought process?”
  *“Where did you **feel uncertain or biased**?”*
- These prompts take seconds but build lifelong cognitive awareness.

Teach Cyber Psychology and Human Factors as a Core Component, Not an Elective

- Introduce concepts like executive control, pattern recognition, and stress performance alongside networking and cryptography; **not after**.
- If students only see “**human factors**” at the end, they **undervalue** them.

Model Emotional Intelligence and Resilience in the Classroom

- Create space for failure, uncertainty, and emotional response to high-stakes simulations.
- **Normalize recovery, not just perfection.**
- This **models the mental habits** students need in the workforce.

Collaborate with Cognitive Scientists and Learning Researchers

- Cybersecurity problems are multi-dimensional and so should be the curriculum.
- Design interdisciplinary modules or co-teach with experts in neuroscience, psychology, or education (that’s people like me ☺).

Seeking collaboration

- I am **volunteering** to provide guest lectures or short courses to teach at least awareness of cognitive skills if you believe your students can benefit from it

Acknowledgements

- Dr. Daniel Shore | Workplace Consultant - Multiteam Solutions
- Subhorup Dasgupta | COO - Indonex Health Analytics Pvt Ltd

References

1. Siddiqui Z. *Casino giant MGM expects \$100 million hit from hack that led to data breach.* Reuters, 5 Oct 2023.

2. Siddiqui Z. *Hackers say they stole 6 terabytes of data from casino giants MGM, Caesars.* Reuters, 14 Sep 2023.

3. Kost E. *What Caused the Uber Data Breach in 2022?* UpGuard Blog, 18 Nov 2024 (incident analysis of Sept 2022 “MFA-fatigue” attack).

4. Kerner S.M. *Colonial Pipeline hack explained: Everything you need to know.* TechTarget, 26 Apr 2022.

5. MultiTeam Solutions. *Stress & Burnout in Cybersecurity: The Risk of a Thousand Papercuts.* Black Hat Europe survey of 173 respondents, May 2024.

6. ISACA. *State of Cybersecurity 2024: Global Update on Workforce, Resources and Budget.* ISACA report, 2024.

7. Hack The Box. *Building a Firewall Against Cybersecurity Burnout.* Censuswide global study, 2024.

8. Devo Technology & Wakefield Research. *2022 Devo SOC Performance Report™ – SOC Leaders and Staff Are Still Not Aligned.* Survey of 1,100 professionals, 2022.

9. Devo Technology & Wakefield Research. *83 % of IT Security Professionals Say Burnout Causes Data Breaches.* Press release, 19 Sep 2023.

10. ThriveDX Media. *Investigating the MGM Cyberattack – How social engineering and a help desk put the whole strip at risk.* 6 Oct 2023.

References

11. National Institute of Standards and Technology (NIST). *Workforce Framework for Cybersecurity (NICE Framework),* SP 800-181. November 2017.

12. Chowdhury N.H., Adam M.T.P., Teubner T. *Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures.* **Computers & Security** 97 (2020) 101931. DOI 10.1016/j.cose.2020.101931.

13. Vishwanath A., Herath T., Chen R., Wang J., Rao H.R. *Why do people get phished? Testing individual differences in phishing vulnerability within an integrated information-processing model.* **Decision Support Systems** 51 (3) 576-586 (2011). DOI 10.1016/j.dss.2011.03.002.

14. Diestel S., Cosmar M., Schmidt K-H. *Burnout and impaired cognitive functioning: The role of executive control in the performance of cognitive tasks.* **Work & Stress** 27 (2) 164-180 (2013). DOI 10.1080/02678373.2013.790243.

15. Greenlee E.T., Funke G.J., Warm J.S., et al. *Stress and workload profiles of network analysis: Not all tasks are created equal.* In **Advances in Human Factors in Cybersecurity** (AHFE 2016), pp. 153-166.

16. Singh T., Johnston A.C., D’Arcy J., Harms P.D. *Stress in the cybersecurity profession: A systematic review of related literature and opportunities for future research.* **Organizational Cybersecurity Journal: Practice, Process and People** (ahead-of-print, 2023). DOI 10.1108/OCJ-06-2022-0012.

17. Wiederhold B.K. *Increasing cybersecurity through emotional engagement.* **Cyberpsychology, Behavior, and Social Networking** 24 (9) 579-580 (2021). DOI 10.1089/cyber.2021.29224.

18. Menard P., Warkentin M., Lowry P.B. *The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination.* **Computers & Security** 75 147-166 (2018). DOI 10.1016/j.cose.2018.01.020.

Questions/connect

My Email

Sateesh.Nutulapati@gmail.com

My LinkedIn QR code

https://www.linkedin.com/in/sateeshnvl/