Partnership for Cyber Security Innovation

Security Behavior Coach: job profile and core tasks

Within the PCSI Security Behavior Coach project, the need was identified for a new security role that would become responsible for the visibility, reduction, and prevention of issues in cybersecurity that concern human actors.

The Security Behavior Coach (SBC) is passionate about understanding why humans do what they do in their daily journeys of getting things done, and connects this understanding to usable security and sound cybersecurity controls. It is a new role within organizations that can complement existing cybersecurity or process management roles.

Would you like to introduce the role of the Security Behavior Coach in your organization? Find out below what type of person would fit the profile and which steps this expert needs to take!

Job Profile

Profile description	An SBC actively contributes to protecting companies against cybercrime and analyses human-induced vulnerabilities in organisational processes. The SBC understands (employee) behaviour and can subsequently steer technical solutions to better suit this behaviour, in consultation with others.
Mission	Analyse work processes from a behavioural point of view to detect issues. The SBC then initiates process improvements, technical improvements or behavioural interventions to minimise cybersecurity risks.
Core tasks	• Analyse and deconstruct processes, assess issues • Monitor and analyse human (behaviour) in processes • Perform data analysis and interpret results • Advise on improvements or behavioural interventions
General competencies	• Combines curiosity with analytics • Empathetic, focuses on cooperation and maintains (informal) networks • Persuasive and assertive, while maintaining good relations • Problem-solving skills and creativity
Job-specific competencies	• Experience in assessing human behaviour and knowledge of end-user cybersecurity • Strategic communication skills to level and interact credibly with stakeholders throughout the organisation • Ability to detract the right information from qualitative and quantitative data • Autonomously build (informal/temporary) teams to pragmatically solve identified issues

Education/previous experience	• At least 5 years' experience in working in (preferably project-based) settings where human behaviour meets technology • A genuine interest in, or affinity with, ICT and Cybersecurity • A university degree in a relevant field (e.g. psychology, industrial engineering and management) • Experience with peer coaching and/or setting up (informal/temporal) communities of practice

Core tasks: step by step

Step	Sub-step	Description	Available resources
Analyse the process	**Gather process information; Gather quantitative and qualitative data on the process**	First the SBC identifies a process that can be improved from a human behaviour angle or that is proposed because of incidents. The SBC analyses this process using instructions, process flowcharts, etc.	• Existing process descriptions • Process analysis template • Journey mapping method
Understand human behaviour and risks	**Conduct interviews and observations with relevant employees and stakeholders; Perform desk research on the process**	Vulnerabilities, threats, incidents and (sources of) behavioural risk. Consider indicators such as high staff turn-over, manual hand-overs, etc	• Problem analysis template • Interview template • COM-B behaviour model
Define (barriers for) target behaviour	**Specify target behaviour and its barriers in detail**	What is the behaviour? Be as specific as possible. Probably there are multiple behaviours that need to be performed for a more secure process. And what barriers stand in the way of achieving this?	• Barrier identification template • BIT tool
Design interventions	**Select appropriate and achievable behavioural interventions**	Consulting and advising on process improvements based on analysis of desk research, interviews and observations	• Intervention template • CASI tool

If you'd like to learn more about this new role, please get in touch with us!

Send us an e-mail for more information: info@pcsi.nl.