The Security Behaviour Coach: Empowering Cybersecurity through People-Oriented Design

Introduction

Most organizations still have a primarily technical view of cybersecurity risks and continue to take an exclusively defensive approach by throwing technology at the problem. But focusing only on technology does not create good cybersecurity. A more integrated approach is needed that takes into account all elements in the cybersecurity system, including people and processes. And balance is needed between these elements to avert incidents. Recognizing this integrated approach, a new role in the realm of cybersecurity had been put forward by the Partnership for Cybersecurity Innovation (PCSI): the Security Behaviour Coach. By addressing the interplay between people, processes, and technology, the Security Behaviour Coach aims to reduce human risk and prevent cyber issues proactively. This contribution explores the significance of this new role.

Understanding Human Behaviour

Many of the cybersecurity incidents that people are blamed for do not originate from the end user, but from other elements in the cybersecurity system. Human errors often arise from flaws in the system design itself. The Security Behaviour Coach acknowledges that humans are an integral part of the cybersecurity system and good system design takes into account people's skills and weaknesses. By discovering how and when humans 'touch' data throughout the working day, the coach can uncover the circumstances in which psychological-related system vulnerabilities may lead to security incidents. Hence, the Security Behaviour Coach applies principles from behavioural sciences to gain insights into why people make certain choices and engage in potentially dangerous online practices.

People-Oriented Cybersecurity Design

While many organizations have security awareness programs in place, these programs often focus primarily on imparting knowledge and raising awareness. However, a system-level approach that considers the balance between people, processes, and technology is crucial. The Security Behaviour Coach fills this gap by integrating human factors into the design of security measures. This holistic approach ensures that security solutions are not only effective but also considerate of the capabilities and limitations of individuals within the organization. Hence, the design challenge to achieve satisfactory cybersecurity solutions requires an interaction where people, process and technology complement each other rather than obstruct each other.

Proactive Risk Mitigation

Rather than solely responding to incidents after they occur, the Security Behaviour Coach seeks to understand the root causes of cyber risks. By identifying and addressing the underlying factors that contribute to risky behaviour, such as poor security culture or insufficient training, the coach works towards preventing incidents from happening in the first place. This proactive stance enables organizations to minimize potential vulnerabilities and enhance their overall cybersecurity posture.

Establishing People-Oriented Design

The Security Behaviour Coach collaborates with various stakeholders, including IT teams, executives, process owners, and employees, to establish a people-oriented design in cybersecurity. This approach encompasses multiple aspects:

1. Technology: The coach works to integrate user-friendly cybersecurity tools and technologies that align with human behaviour. This includes implementing intuitive interfaces, human-centred authentication mechanisms, and automated security measures that minimize the burden on end-users. By introducing usable security controls that support the goal-oriented behaviour of employees (i.e. getting the work done), organizations can reduce the likelihood of human error and compliance issues, leading to risk exposure and security breaches.
2. Policies: The Security Behaviour Coach contributes to the development of comprehensive cybersecurity policies that consider human factors. This involves establishing guidelines, procedures, and protocols that promote usable security controls and align with the organization's culture. By clearly outlining expectations and consequences, policies become an essential tool for shaping employee behaviour in a security-conscious manner.
3. Culture: A security-conscious culture is vital for mitigating cyber risks effectively. The Security Behaviour Coach works with organizational leadership to foster a culture that prioritizes cybersecurity. This includes promoting open communication, encouraging reporting of potential vulnerabilities, and creating a supportive and friendly environment where cybersecurity is everyone's responsibility. By integrating cybersecurity into the organizational culture, human risk can be significantly reduced.
4. Behaviour Change: The Security Behaviour Coach employs strategies to influence positive behaviour change across the organization. By leveraging behavioural insights, the coach implements tailored training programs, engaging awareness campaigns, and incentives to

encourage individuals to adopt cybersecure practices. Regular assessments and feedback help track progress and ensure continuous improvement in cybersecurity habits.

Benefits and Implications

Integrating the Security Behaviour Coach role into organizations brings numerous benefits. Firstly, it enables a proactive, more strategic approach to cybersecurity, by addressing the root causes of cyber risks. By focusing on human risk, organizations can reduce the likelihood of incidents, minimizing potential financial, reputational, and operational damages. Moreover, a people-oriented design in cybersecurity cultivates a sense of ownership and responsibility among employees. By involving individuals in the design of the cybersecurity system and providing them with the necessary knowledge and skills, organizations create a collaborative defence against cyber threats. This collective effort not only enhances the overall cybersecurity posture but also fosters a culture of vigilance and resilience.

Pilot Test

In a pilot test of this new role, investigating cybersecurity risks in a wholesale banking app verification process, it was found that banking employees sometimes skip required telephone calls to legal representatives. An analysis of the Security Behaviour Coach, after conducting interviews with employees and workplace observations, showed that the phone anxiety (telephobia), especially when employees have to talk to persons in executive-level positions, caused this omission to perform the required security check. Consequently, the Security Behaviour Coach suggested process changes to the process owner. For instance to allow employees to use text messaging instead, to lower the human risk of employees omitting required process steps and, hence, make the verification process more cybersecure.

Technology transfer

In order for society and business to benefit from this innovative cybersecurity role, we translated our applied research results into a practical application in the outside world: a blueprint for a training course. SECO institute and Security Academy have taken up the gauntlet to develop, with our help, a new foundation and practitioner course to address the job role of the Security Behaviour Coach.

Conclusion

In the face of evolving cyber threats, the Security Behaviour Coach plays a vital role in establishing a people-oriented design in cybersecurity. By incorporating human factors into security practices, organizations can address the root causes of cyber risks and empower employees to make secure choices. Through technology, policies, culture, and behaviour change, the Security Behaviour Coach transforms cybersecurity from a reactive approach to a proactive, strategic, and human-centric endeavour. To conclude, the PCSI hopes that this new role will quickly find its place in practice and challenges you to play a part of this transition to a new integrated approach to cybersecurity.

Partnership for Cybersecurity Innovation (PCSI)

Partnership for Cyber Security Innovation

The Partnership for Cyber Security Innovation (PCSI) is a Dutch public-private partnership and plays an essential role in a secure and resilient digital society by innovation in the field of cybersecurity. PCSI joins forces in developing applicable and innovative cybersecurity solutions that companies and organizations in Dutch society can use to protect themselves against tomorrow's cyber-attacks.

Dr Rick van der Kleij

is an expert in the field of human factors with a keen interest in cybersecurity. His expertise lies in the sub-discipline of psychology that focuses on the link between human behaviour, engineering, and computer science. He strongly believes that a holistic approach to risk management is essential for ensuring cybersecurity and that organizations should adopt a socio-technical or human-centred cybersecurity approach. Rick works at TNO and is a project leader of PCSI. Rick is also a member of the advice committee of the Security Awareness NL foundation.

External links

- https://pcsi.nl/
- Security Behavior Coach | Projects (pcsi.nl)
- NLSecure[ID] - Rick van der Kleij
- From Security-as-a-Hindrance Towards User-Centred Cybersecurity Design

Contact

info@one-conference.nl one-conference.nl