Behavioural aspects of cybersecurity

Technical cybersecurity measures do not exist in a vacuum and need to operate in harmony with people. Against this backdrop, ENISA publishes a report comprising four evidence-based reviews of human aspects of cybersecurity: two based on the use and effectiveness of models from social science, one on qualitative studies, and one on current practice within organisations.

Published on April 16, 2019



© Copyright: Shutterstock

Tagged with

* [cybersecurity](https://www.enisa.europa.eu/search?Subject%3Alist=cybersecurity)

In summary, ENISA found a relatively small number of models, none of which were a particularly good fit for understanding, predicting or changing cybersecurity behaviour. Many ignored the context in which much cybersecurity behaviour occurs (i.e. the workplace), and the constraints and other demands on people’s time and resources that it causes. At the same time, there was evidence that models that stressed ways to enable appropriate cybersecurity behaviour were more effective and useful than those that sought to use threat awareness or punishment to urge users towards more secure behaviour.

The report offers recommendations for specific groups such as policy makers, management and organizational leaders, CISO and security specialists, CSIRT / CERT community, software developers and awareness raising managers.

ENISA proposes that practitioners can take significant steps towards helping employees to act in a more secure way. This may involve skills-based training and support but may also require the restructuring of security practices and policies, to better align with people’s workplace goals and/or capabilities. ENISA proposes a model of awareness, analysis and intervention for organisations to systematically plan and implement changes to address human aspects of cybersecurity.

For policy makers, ENISA identified a clear lesson from the reviews - increasing cybersecurity literacy and skills is an evidenced method to support citizens to protect their cybersecurity.

Management and organisational leadership need to shift their perspective on what their role and responsibilities are in managing cybersecurity in their organisations. They should decide which security risks they want to manage, and commit the resources required.

CISOs and security specialists need to know the impact that security policies can have on staff in daily business operations. They need to be visible and approachable and even acquire the ‘soft skills’ to do this effectively, ideally through special programmes.

Incident response teams and security operations centre staff should be enabled to perform in the fight against cyber threats. Their employers need to ensure sufficient staffing levels, invest in training and personal growth, and support innovative approaches such as team and multi-team.

Last but not least, all people involved in cybersecurity should mainly aim to provide users with the skills in order to cope with cyber threats rather than running repetitive awareness campaigns on the scale and vulnerability of cybersecurity threats.

For the full report: [Behavioural aspects of cybersecurity](https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity" \t "_self)