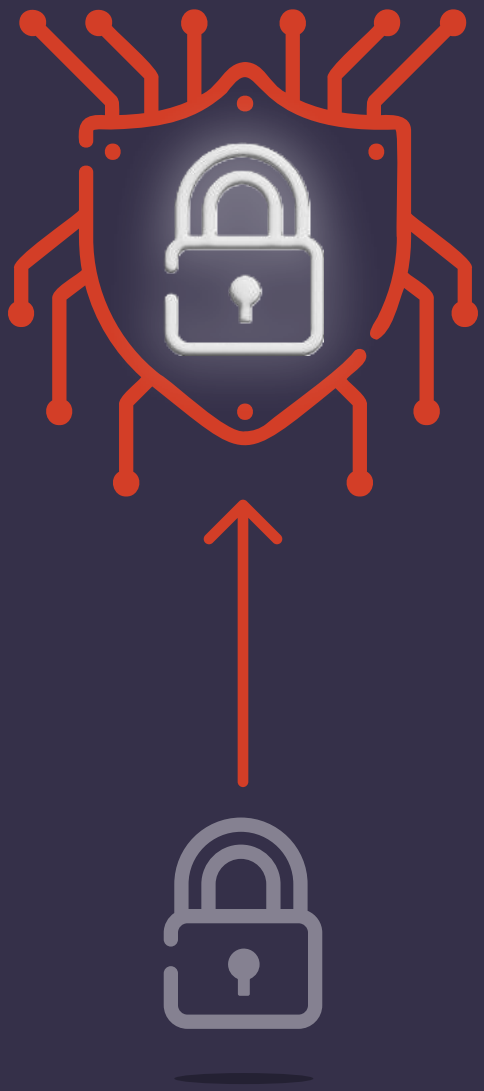


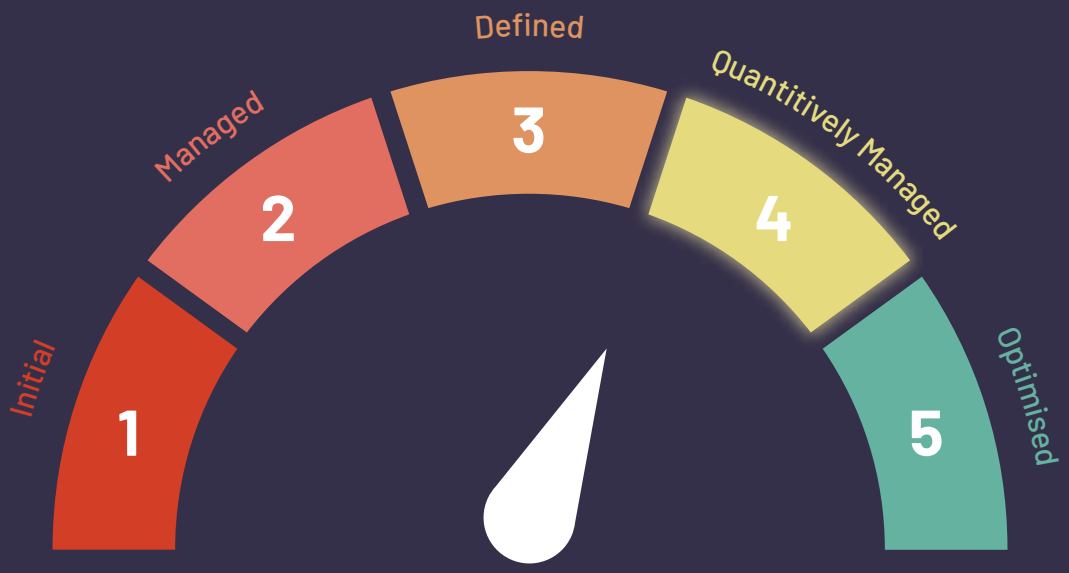
From Quantitively Managed to Optimised

Improving Cyber Security Behaviours in Your Organisation

MetaCompliance®

HOW DOES YOUR ORGANISATION MEASURE UP?

The results are in, and your organisation has scored **4.0/5** on the Cyber Security Behavioral Maturity Model.



4.0 out of a possible 5

DIAGNOSIS - YOUR SCORE CATEGORY IS QUANTITIVELY MANAGED

Your organisation is taking advantage of automated Security Awareness Training which helps to provide consistent and scalable training to employees, reduce the risk of human error in security breaches, and comply with regulatory requirements.

Your organisation has a structured and standardised approach to managing its cyber security risks by aligning to a security framework. Aligning with a security framework demonstrates to your customers, partners and stakeholders that your organisation takes cyber security seriously and has implemented appropriate controls to protect sensitive data.

Your organisation tailors Security Awareness Training according to specific threats. Doing so provides a better understanding of the real-world risks that could compromise your organisation's security. By addressing specific threats, employees are better equipped to identify and respond to potential security incidents, and the organisation can reduce the risk of a cyber attack.

Cyber security training is an ongoing effort in your organisation all year round. Regular training helps to reinforce positive cyber security behaviours and ensure that employees remember and apply the information they have learned.

By customising cyber awareness training to align with the roles and responsibilities within your workforce, your organisation imitates the same tactics employed by cybercriminals when targeting specific groups within an organisation. This approach personalises the training experience, making it more relevant and impactful for each individual.

Your organisation delivers cyber security training in the native language of the learners. This ensures that they have a deeper understanding and connection to the material, leading to better engagement and retention. Adopting a people-centric approach to information security, and incorporating localised training programs in the language of end users, can greatly enhance the success of your organisation's security awareness efforts.

Our recommendations provide practical advice to nudge your organisation towards better cyber security practices, equipping employees with the knowledge they need to protect your organisation against cyber threats. By implementing the right tools and processes now, these recommendations can help reduce the risk of costly cyber attacks and minimise human error.

STARTING SMALL, THINKING BIG: PRACTICAL RECOMMENDATIONS FOR EFFECTIVE CYBER SECURITY AWARENESS TRAINING

Organisations with an 'Quantitively Managed' security awareness program score should focus on delivering in the following areas:

ENCOURAGE END USER FEEDBACK

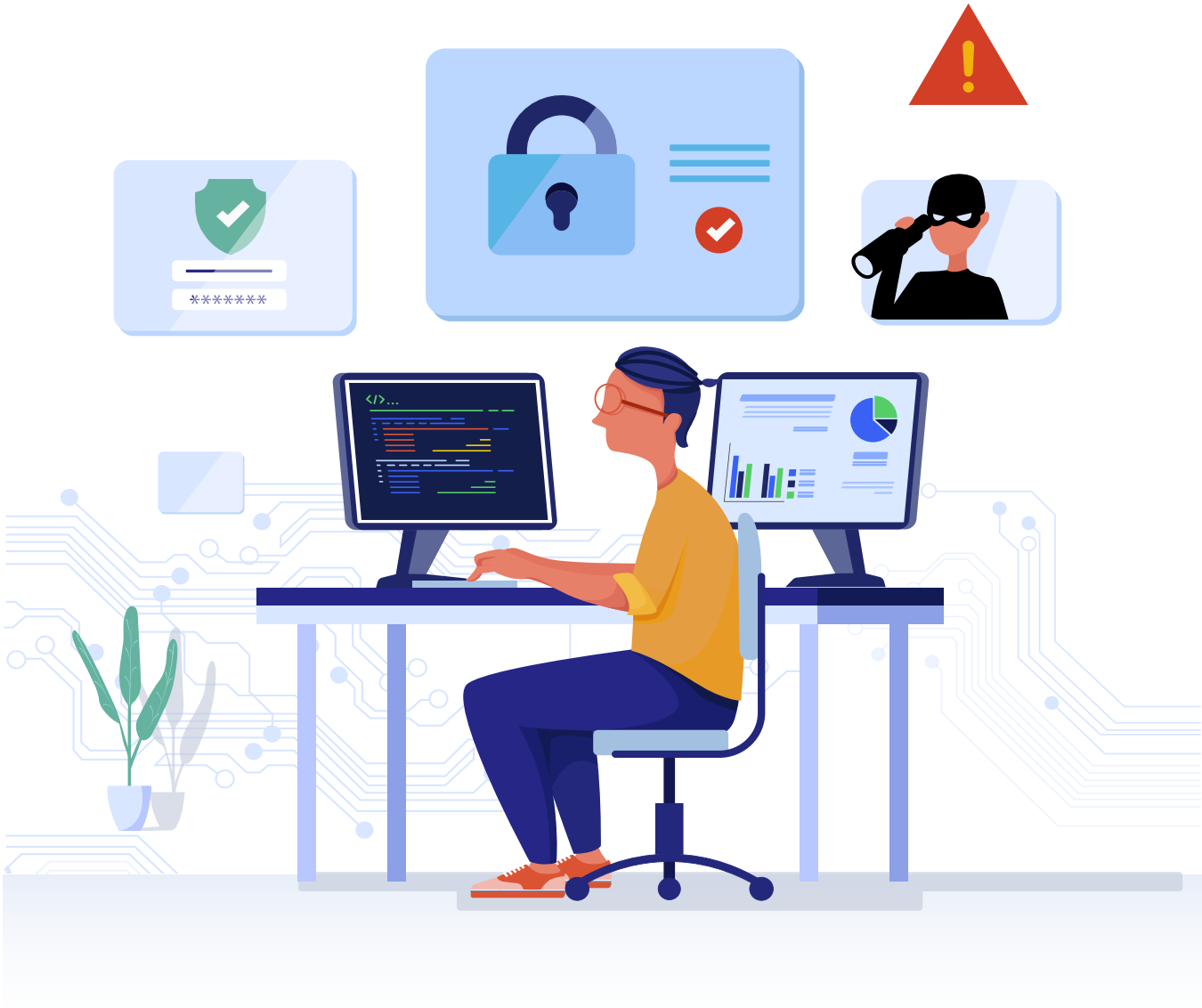
Encouraging end users to share feedback about your organisation's cyber security training program can help to improve future awareness training programs, increase employee engagement, measure the effectiveness of the training, and empower employees to take ownership of the program.

CONDUCT REGULAR REVIEWS

Measuring the success of a security awareness program is essential to assess its impact and effectiveness. The results of this can highlight areas for improvement and demonstrate the program's positive impact on employees' behaviours. This information can be used to justify the investment in Security Awareness Training and strengthen executive support for future initiatives.

USER GENERATED PATHWAYS

Enabling users to generate their own learning pathway, according to their content preferences allows individuals to tailor their learning experience to their specific needs and interests. Self-directed learning offers benefits such as greater flexibility for the end user, as well as increased engagement and retention.



MAXIMISE THE SUCCESS OF YOUR SECURITY AWARENESS PROGRAMME

Your cyber security awareness culture is too important to leave to chance.

To learn how MetaCompliance can help you to implement a best practice security awareness program and improve cyber security behaviours within your organisation, **schedule a complimentary consultation with our employee engagement specialists at www.metacompliance.com.**