


Implementing an

Optimised Cyber Security Training Program

in Your Organisation

Table of Contents



Assessing your awareness levels and setting the right direction for success	1
How does your organisation measure up?	2
Initial, Managed	3
Defined, Quantitively Managed	4
Optimised	5
Practical recommendations for optimised cyber Security Awareness Training	6-10
Maximise your success	11

Assessing your **Awareness Levels** and Setting the Right Direction for Success

What is **it?**

Our Cyber Security Behavioural Maturity Model is a comprehensive measurement tool designed to revolutionise the way you assess your organisation's security awareness program.

The Security Awareness Maturity Model enables you to evaluate the current maturity level of your program and benchmark it against industry best practices.

By answering a short assessment, you can determine your organisation's maturity score and gain invaluable insights and recommendations for improvement. With our model, you can consistently measure your awareness levels over time, ensuring a proactive approach to security.

Additionally, our tool empowers you to identify the reasons behind any gaps in your awareness program's effectiveness and devise a strategic roadmap for continuous improvement. Leverage the power of our Security Awareness Maturity Model to effectively communicate the value of your program to senior leadership, ensuring their support and investment in your organisation's cyber security initiatives.

Take charge of your security awareness journey today and unlock a new level of cyber resilience.



Is **your** security awareness program on point?

[Audit your training](#)

Click to discover your score

So...

How Does Your Organisation Measure Up?



The Security Awareness Maturity Model consists of **5 results**, ranging from **'Initial'** to **'Optimised'**.
The results are defined as follows



1. INITIAL

Currently, cyber security is the responsibility of your IT Department, and there is no dedicated resource for training your employees on best practice behaviours.

Not having support from the senior leadership team to improve cyber security awareness can have serious consequences for your organisation.

Without senior leadership support, employees may not understand the importance of cyber security and become unmotivated to follow best practices.

This can result in a lack of adherence to security policies, increased vulnerability to cyber attacks, and ultimately, loss of sensitive data, financial loss, and reputational damage.



2. MANAGED

The information security function has ownership of cyber security awareness, and there is clear responsibility for this crucial aspect of the organisation's security posture. Having an in-house security team provides clarity and allows for a more tailored approach to identifying the most pressing threats to your business.

Your organisation emphasises that security is everyone's problem, and it is a key concern for your C-Suite.

A positive tone from the top has helped to lead the change in attitude throughout the entire organisation towards the importance of security. C-level support provides the backbone needed to build a culture of security awareness.

Your organisation has already taken steps to enhance its cyber security posture and recognises the importance of ensuring that employees are engaged in Security Awareness Training.

You have laid a solid foundation by implementing various cyber security training best practices, which is commendable in today's rapidly evolving threat landscape.

3. DEFINED

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 makes Security Awareness accessible and engaging for a diverse workforce. Offering training materials in your employees' native language and preferred format, helps comprehension and retention of the content, which can ultimately lead to better results.

Key cyber threats are covered within your Security Awareness Training program, however, cyber security initiatives are still a technical problem and are not aligned with business priorities. All employees, from executives to entry-level staff, have a role to play in protecting your organisation's information and systems.

4. QUANTITATIVELY 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 makes Security Awareness Training accessible and engaging for a diverse workforce.

Offering training materials in your employees' native language and preferred format, helps comprehension and retention of the content, which can ultimately lead to better results.

Key cyber threats are covered within your Security Awareness Training program, however, cyber security initiatives are still a technical problem and are not aligned with business priorities.

All employees, from executives to entry-level staff, have a role to play in protecting your organisation's information and systems.

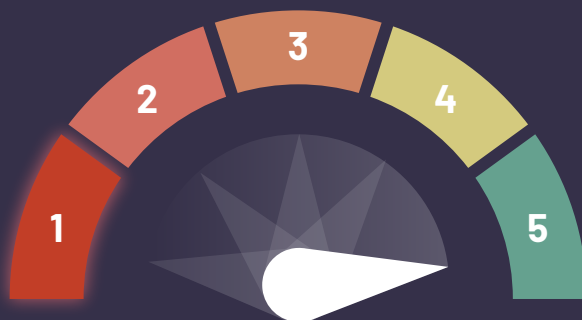
# 5. OPTIMISED



Your organisation has diligently implemented the key practices to create an optimised Security Awareness Training program.

By incorporating comprehensive security measures, your organisation has built a strong foundation to mitigate risks effectively.

However, even in the face of constant advancements in cyber threats, there is always room for continuous improvement. By maintaining these recommendations, your organisation will stay at the forefront of cyber resilience and remain well-equipped to tackle emerging threats.



Ready to level up your security awareness program?

[Audit your training](#)

*Click to discover  
your score*

our..

Practical Recommendations for  
**Optimised Cyber Security  
Awareness Training**





## Secure C-Suite support

If you want to effect change, you have to get buy-in from the right people to do so. Security is everyone's problem, including at the board level.

A positive tone from the top helps to change the attitude towards security that filters through the entire organisation. C-level support provides the backbone needed to build a culture of security awareness.



## Dedicated resources and domain expertise

One of the key steps in strengthening your security program is the appointment of a dedicated team or individual to manage cyber risk and promote security awareness within your organisation. Having an in-house security team provides clarity and allows for a more tailored approach to identifying the most pressing threats to your business. With the ever-evolving nature of cyber threats, it is crucial to have a dedicated resource in place.



## Deliver departmental and relevant training

By customising cyber awareness training to align with the roles and responsibilities within your workforce, you can imitate 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.



## Localised learning

Effective Security Awareness Training must be delivered 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.



## Tailor training to specific threats

In creating an effective security awareness program, your organisation needs to evaluate the threat landscape and identify your top risks. Doing so provides a better understanding of the real-world threats 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.



## Automate your security awareness training

Automating your Security Awareness Training program can bring significant benefits, just as automation can improve other business processes. This can streamline the creation and delivery of your awareness program, freeing up resources for other tasks. Automation can also manage the ongoing maintenance of the awareness program, ensuring that the training remains current and effective throughout the year.



## Embed awareness all year round

Training employees about cyber security should be an ongoing effort as the threat landscape is constantly evolving. New security risks and threats are emerging all the time, and employees must stay up-to-date on the latest techniques. Regular training also helps to reinforce positive cyber security behaviours and ensure that employees remember and apply the information they have learned.



## Follow a security framework

A security framework, such as NIST or ISO27001, provides a structured approach for identifying, assessing, and mitigating risks to your organisation's assets, information, and systems. It ensures consistency in security practices and reduces the risk of human error. Implementing a security framework also shows the organisation's dedication to both internal security and to external stakeholders.



## Focus on different formats

Organisations should provide cyber security training in different formats to cater for the diverse learning styles and preferences of their employees. Not all employees learn in the same way, and a variety of training formats can help to reach a wider audience and ensure that the training resonates.

Some employees may prefer interactive eLearning courses, while others may prefer gamification. By offering a range of training options, organisations can engage employees more effectively, increase participation and ultimately improve the overall impact of the training program.



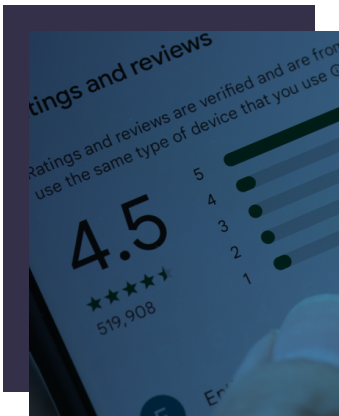
## Implement multi-channel delivery

Many organisations struggle to engage users to complete any type of training. The key is to choose the path of least resistance and make it easy for employees to engage. By allowing users to complete their training within their preferred platform, such as Microsoft Teams or Slack, user engagement is improved, participation rates are higher, and the resistance to training is reduced.



## Encouraging 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 positive impact of the program 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 to implement a best practice security awareness program and improve cyber security behaviours in your organisation, schedule a complimentary consultation with our employee engagement specialists at [www.metacompliance.com](http://www.metacompliance.com)