Q&A Summary from **MetaRisk Webinar** – 29/05/24

Here's what you asked …

Q: Can we provide users with context for their risk score (e.g., if 80 is good or bad)?

A: Yes, by enabling the end user dashboard, users will see their risk score out of 100, accompanied by a visual indicator like "High" for a score of 80.

Q: Can we use our organisational domain for phishing simulations?

A: Yes, you can add and verify a domain that you own on the platform. However, we strongly advise against using your corporate domain for phishing emails.

For more information and best practice for using this feature, check out our Customer Custom Phish Domains guidelines here.

Q: Is there functionality to crop existing Nanos?

A: The Creative Team is open to reviewing any requests for cropping or removing content from existing Nanos. Contact your CSM Representative for more assistance on how we can personalise these features for you.

Q: Can we see both English and English-US Nanos when creating a course?

A: We are looking into providing a unified selection of Nanos regardless of the selected language. Once this is established, we will endeavour to communicate this with all our clients.

Q: Can the Intro/Outro on courses be made optional?

A: We are examining the possibility of making Intro/Outro optional to improve user experience. Once we've established this option, we will let our users know.

Q: When will MetaCompliance Symphony be available?

A: Based on customer feedback during Symphony's beta testing, we decided to remove some features that weren't as beneficial as initially thought. However, exciting features like the Employee Risk and Engagement Dashboard, a major component of Symphony, have been integrated into other offerings that will be made available for customers in June 2024.

Q: Will there be content on using AI safely?

A: Yes, we are releasing AI-related content quarterly, covering threats like data leaks and deep fakes, and guidance on formulating AI policies. You can keep up to date with "what's new" and updated features within our Customer Portal.

Q: Should we deploy the MC Report button if we already have the Microsoft Report message button?

A: Yes, deploying the MC Report button positively impacts a user's risk score. You can find more information on this here.

Q: Do you have more details on new/upcoming interactions?

A: We are developing scenario-based interactions on core cyber risks which will put the learner in the shoes of someone facing a challenge - Our first planned interaction will be on Access Control which will be launching in Q2.

Q: Can we avoid showing version numbers on modules, to users?

A: We are looking into simplifying titles and removing version numbers to make them more user-friendly.

Q: Will there be targeted content for specific segments like Automotive?

A: We are not currently releasing content specifically for the Automotive industry, but if this is something you feel would be beneficial for your organisation, we advise speaking to your CSM representative who can advise you further on the next steps.

Q: Can course emails come from an internal email address to avoid phishing concerns?

A: You can mask the email address to make it more familiar for your users. We also advise using the MyCompliance Teams App (if you use teams) for notifications – Follow our guidance here.

If you have any more questions, please feel free to reach out to Mairead directly at mcosgrave@metacompliance.com