*Thank you for attending the '**From Paper to Practice: Communicating and Implementing your Cybersecurity Strategy**' webinar by CRMG and Layer 8. Below are questions from the audience that were unable to be answered due to time running out. CRMG and Layer 8 have provided detailed answers. Please note that the answers given represent the individual views of both organisations who have significant experience in cyber risk and/or business culture.*

*We hope this is helpful, and for any further questions please contact us at **info@crmg-consult.com** or* enquiries@layer8ltd.co.uk.

Questions

1. **We have a security champion's programme, but most people were unwillingly volunteered, and we find it difficult to get their time and attention. What tips do you have?**

Being volunteered rather than volunteering is the number 1 reason we hear for champion's programmes not working. We recommend getting buy in to the programme by making it resonate with people's core values and giving them the opportunity to develop how the programme will be delivered. Simple things like allowing the group to collaborate on what they are called, and some of the tasks they will carry out – this can be very powerful. Additionally, the job of the person leading the champion's programme should be a 'creator of opportunity' for the champion's, rather than exclusively teaching them about security. What we mean is, if the champions are given opportunities to develop their core skills (communicating with impact, being influential etc) and given chances to demonstrate their learning in front of senior manager, then the programme is seen as good career development and personal learning, at the same time as helping to raise the profile of security and change employee behaviours.

2. **We already know that people have a fairly negative perception of security, how can we start to change that?**

The obvious immediate response is to find out why. Is it the way the people talk about security? Is it that some of the restrictions put in place are too aggressive, or misunderstood? A quick win to kick start this process is by making a few changes to help some of the main challengers you have here. Is there something you or your team can do for them that might change their opinion? Can you create a success story from it? Can you encourage that person to share the story with others?

3. **Do you have any examples of pictures to illustrate security awareness for staff that hit the spot?**

Making an impact is quite personal and for true impact it must hit an emotion. Which is why short, meaningful videos are very effective in getting people to pay attention. Keep in mind that the topic that 'hits the spot' for one person might be different to that of another. Here is a link to a show reel of some videos we recommend. If there's one you'd like to see in full get in touch and we'd be happy to share it:
https://www.youtube.com/watch?v=GXKWIF4Ih3w&list=PL5bnu_ccSbIY23Fi9uO94qtFS5CIbp29Z

4. **I need to get buy in for a new web-filtering technology. I tend to go into the Boardroom and present stats of all the breaches and fines to help win a case. How could I turn that into a more positive message?**

Have you ever tried creating a provocation? Provocations are a great way to present a case for something in a really impactful way, in around 3-5 minutes. A bit of research needs to be done beforehand to establish a business challenge (outside of security) that will immediately resonate with the audience you will be presenting to. It then demonstrates a bold vision for how the security initiative can support the success of that particular business challenge. We attach a link to a document that gives more detail of the process of creating an impactful provocation.

5. **I gave a presentation for a previous organisation during an interview that showed how crucial it was for everyone in the organisation to be empowered and be part of the conversation in cybersecurity. The Head of IT looked at me with horror- I was going to empower staff across the company in cybersecurity? I wasn't hired, and it was no doubt about the 'people' stuff. How do we overcome this?**

Changing the mind of someone who in general is not a person who is open to others' opinions is hard. So, don't try and convince them, they probably like the challenge of an argument. This type of character responds better if they think they have made a conscious decision. One method is don't try and convince them, they need to convince themselves. The best way of getting someone to convince themselves is to ask them a series of questions that make them question their logic. For example, tell me about the biggest challenge you have protecting the IT Security of this business? How do staff use IT at the moment? Do you expect your employees to be self-motivated/empowered to drive the success of your business commercially? Does the use of IT help your business and employees be more successful commercially? How would you expect an employee to respond to a customer if they asked their opinion on cybersecurity? You will need to create some questions that resonate well with the person you are talking to.

6. **Do you think that cybersecurity Teams have sufficient sway (i.e. power at Board level) to drive a change in the culture of conversation to drive the cyber risk agenda?**

To answer the question generally, some Cyber Teams do, and some don't. However, whilst it's preferential to start the conversation at Board-level, there are ways to get to the Board via stealth methods. An organisation that we work with was already pretty wise to the fact that talking about culture at Board-level would probably be fruitless because the organisation considered they had bigger fish to fry, so they started conversations with key process owners that already had most influence with the Board. They were able to establish some areas that security could help that process owner achieve what they needed to, and thus through 'facilitated' stealth get the message to the Board. They never asked to go to the Board meeting, but instead found themselves being invited when the Board started hearing about what good was happening.

7. What is the best way to prove a ROI on your investment in security culture?

As we discussed in the masterclass measuring change has been notoriously difficult. Often this is because we find ourselves trying to develop a formula or equate it back to numbers and percentages (because we think that is how people want to see it presented). However, trying to find a statistic for the effect of a positive culture can appear meaningless, because they tend to represent indicators or what might happen. What we actually want to measure is what IS happening and HOW it's making a difference. So first we need to understand very specifically WHAT habits and behaviours will make a positive impact on the business. And then find a way of seeing whether they are happening. Let me give an example, we would use objectives and key results (OKIs) rather than KPIs. Objective might be - increase ability for all customer facing employees to discuss information and cybersecurity with customer and supplier. Key results might be (reduction in total time Security Team spends supporting customer facing staff to have basic conversations with customer. Increase in number project where security has been considered. Etc. In terms of measurement and ROI for culture we need to think differently. We don't need to measure an exact number or turn it into a complex formula. Let's find some good stories through our champion's and network to demonstrate where it's working. This qualitative data will be much more meaningful than an arbitrary number to try and prove ROI.

8. Competence and confidence indexes were mentioned, how do you know whether these are "correct"?

One of the key challenges when you survey people is knowing categorically whether people have answered truthfully or in the way that they think they should be answering. We always recommend following up a survey with some targeted focus groups. It can provide richer data about why people have answered in a certain way and iron out any inconsistencies with how people have answered the questions. We typically find only a small difference between the survey results and the focus groups. The difference being slightly more noticeable in an organisation that has a dominant fear or blame culture. A survey really should be taken as a temperature check rather than an absolute and used to find the areas that come our strongest and then used to help improve areas that need more attention.