MOHAMMAD FIRDAUS JUHARI *Head of Digital Security, Edotco Group*
LinkedIn: https://www.linkedin.com/in/firdausjuhari/

Cyber security leader with years of experience financial, consulting, IT and telecommunication industries. Immense passion in transforming businesses into the next level of cyber-resilience.

TIP 1. CYBER AWARENESS IS A MARKETING JOB

This is one of the areas in cyber security that you need to be least technical, but you must be very good at marketing. You need to make a cyber security message that sounds and looks fun, or nobody will ever listen to you. It is all about engagement, channel management, viewership, and program management. Study your audience and company's culture; then you will get the idea for the best awareness campaign.

TIP 2. RISK UNDERSTANDING IS CRUCIAL

Every business comes with a different cyber risk profile, and this is true all the time. You need to have a solid understanding of what are the threats relevant to your business before investing in people, process and technology. This will help you to establish focus areas in your cyber security strategy, rather than trying to treat all cyber risks as the same.

TIP 3. RECRUIT THE RIGHT PEOPLE

Recruiting cyber security talents can be a bit tricky but, fundamentally, you need the right people for the right position. Cyber security is a broad domain that every position requires different degrees of technical and soft skills. Certifications do not tell the whole story about a candidate. You need to listen to their stories, seek their passions in the stories and know their potential.

TIP 4. KNOW THE GROWTH MARGIN

You must know the extent of growth of every single member of your cyber security talent. Understand their career aspirations and always provide the opportunities for them to grow. Recruiting talent without a growth margin can be a wrong step for your cyber security program as it will add stagnation to your program, or eventual failure

TIP 5. MANAGE MENTAL HEALTH

Cyber security comes with lot of uncertainties mainly due to fast-changing threat and regulatory landscapes. These uncertainties are stress-inducing; knowing how to balance the work and life of your cyber security talents is important. Provide some spaces for your cyber security talents to enjoy their lives. Healthy relationship and work environment matter. In the end, we're all humans!

TIP 6. LEARN FROM INCIDENTS

No business wants to be struck by security incidents, but the good news is that incidents are your lesson opportunity. Your business' cyber security capabilities grow when you learn from incidents and address the gaps that had caused the incidents to happen. Ability to deal with incidents is what makes business more cyber-resilient.

TIP 7. UNDERSTAND CERTIFICATION

Only consider cyber security certification for your company when it is required by the market or provides business advantages. Certification takes lot of effort and absorbs a significant amount of your cyber security team, which might distract them from more important matters, such as incident preparedness. Without a strong reason for certification, it is sufficient to focus on the alignment with best practices.

TIP 8. GET THE POLICY RIGHT

Your security program is driven by your cyber security policy, hence you have to get your policy right before you push your security agendas. Not everything that you read in the textbook is applicable for your business. Make sure your policy makes sense for your business; and it has to be simple and clear for everyone in your company to understand.

TIP 9. BUY TECHNOLOGY THAT MATTERS

Technology is one of the important parts in strengthening your cyber resilience; but any security technology or service that you buy must strictly resolve a gap or problem. Do not buy a security technology simply because others are buying it. By example, do you really need a third party DLP (Data Loss Prevention) solution, or you can live with existing DLP solution in your Microsoft E5 subscription?

TIP 10. VENDORS ARE PART OF YOUR ECOSYSTEM

When your cyber security team is small or maybe inexistant, security vendors are your partners. You need to create an ecosystem of vendors that works for you. You must clearly identify the vendors that are strategically and tactically important for you. Vendors that can be there for you in critical moments such as incidents. Another point to remember, cyber security talent pool is small so that you can also tap on the talents from your vendor to get the best result for your security program.