The Cybersecurity Boredom Fence

Mark Johnson

Cyber Security Advocate

Let's make cybersecurity interesting again!

Do you know why there might be over a million alleged vacancies in cyber security positions worldwide? Perhaps it's because in our efforts to establish a common framework for security, we accidentally built a **boredom fence**. Security is a **culture** based on threat awareness, assessment of risks, and common sense; it's not a list of guidelines, or a philosophical position, and sometimes the only correct answer is the one that works. With a fence this forbidding, with the endless jargon, only a tiny minority of the new recruits we need will ever apply.

I am currently reading yet another version of the 'common body of knowledge' (or CBoK in business jargon) as I belatedly work towards my third certification, and a realisation is dawning. It's actually possible, if you work really hard at it, to take an immersive domain like cybersecurity, and make it so dry that even someone with 30 years' experience in high-tech crime control is falling asleep after ten minutes' reading. Is it only me who feels this way? Somehow, I doubt it…

Engage your audience. Cybersecurity can be exciting!

info@trmg.biz

Where are the stories? Where are the scenarios and the case studies? Put a good one on page one. And another on page five. And on page ten. Human beings were involved in that 'failure of confidentiality', so why not talk about them? Where are the humans in the OSI model? Someone had a motive; what drove them? Someone blundered. Why? Others had something to lose; how did the ‘incident’ affect them?

Remember those 'availability' issues the previous month? Hundreds of thousands of people didn't get paid on time. And that attempt to target critical national infrastructure? The true threat was existential, while the ramifications were dystopian in nature; the stuff of Hollywood blockbusters. So why do we struggle to make these accounts engaging? We need to learn to become good story tellers.

Cyber technology is embedded in our lives and cyber incidents impact on us all at a personal level in some way or another. That’s the missing link; going beyond Business Impact Analysis to Societal Impact Analysis, to Personal Impact Analysis, and to the many engaging tales that flow from such analyses.

Real people with real lives, real ambitions and real responsibilities are affected by cybercrime. Cybersecurity professionals strive to protect those people. Tell your users your human stories too; the late nights and the sweat. You are #cyber-superheroes, so use your powers to pull the would-be crime fighters and the people with a social conscience into the domain. This is what cybersecurity is actually about and this is where the message and the learning need to focus, not on memorizing the XYZ Act of 1956. Put that in an Appendix; it’s enough for most of us simply to be aware of each law’s existence and its relevance in our particular jurisdiction.

Tell the human stories and tell them well. (#cybertales). Draw the audience close around the campfire. Evangelise them **and then ask them** what kind of controls make sense in the face of this or that intriguing risk. You'll be surprised by their ability to think laterally and by how quickly they list almost everything in the CBoK for you, even if they get the jargon wrong. Focus on the principles, on the reasoned thinking, on common sense. After all, the thing about any Common Body of Knowledge is that it’s common knowledge primarily because it **is** common sense.