# A-C of Cyber Security

**Karen Renaud, University of Strathclyde, Scotland (www.karenrenaud.com)**

I have gained inspiration from the Human Factors in Diving[1] community to start an "***A-Zs of cyber security***".

**A: Awareness**. Whenever security professionals talk about cyber security, they bemoan the lack of awareness. This assumes that the only way to get people to behave more securely is to narrow the knowledge gap i.e., "*if only they knew, they would act securely*".

Many awareness raising efforts do their best to deliver the information people need, but they fail to appreciate two important truths:

(1) **Information is not the same as knowledge**. Many impart information, but attendees seldom get an opportunity to apply their new insights. For information to become knowledge, they need to convert information to knowledge: the ability to apply the information, and knowing when to do this.
(2) **Situational awareness is key.** This starts with *sensory awareness* – what we see and hear. The mind then attempts to *make sense* of what they see and hear based on their previous experiences. Note the word "experiences" – not merely information that they have been exposed too – but *experiences* in applying the information. The final step builds on this sense-making to predict the future: to *anticipate what might happen next* based on the actions they decide to take.

    This means that merely imparting information to employees and checking an awareness-raising box is suboptimal. Awareness is necessary but not sufficient.

Awareness efforts *must* give people the opportunity to apply the information and to develop new skills. This will close the knowledge gap and also improve situational awareness, which will have been honed during experience-building training exercises.

**B: Briefing**: many consider that they have briefed employees during awareness raising endeavours. The kind of briefing that few engage in is related to giving people sufficient information to enhance their just-in-time situational awareness. For example, one employee might spot a phishing message and report it to the security officer. The officer might send an email to warn all staff about the Phishing message. Employees are likely to see the warning *after* they have opened the rogue email. There is a need for another channel to ensure that people are warned *before* they process the Phish email. Of course, the security officer might be able to remove the email from all the employees' inboxes, but that also misses a valuable opportunity to create a learning experience. It might well be preferable to forewarn and forearm employees, using a different channel. This allows them view the Phish

[1] https://www.hf-in-diving-conference.com/

This is a peer-reviewed, accepted author manuscript of the following article: Renaud, K. (2021). The A-Z of cyber security: A-C of Cyber Security. Network Security, 2021(11), 20. https://doi.org/10.1016/S1353-4858(21)00134-3

email knowing exactly what it is. This builds those experiences that they can rely on to enhance their day to day situational awareness.

**C: Communication**: briefing is related to effective communication. The sender of any cyber security related message has to be aware of: (1) the recipient's likely response to the message based on the language and terminology it uses, and (2) the emotions it is likely to elicit. In terms of the first, keep it simple and don't use acronyms. Make it actionable: tell them what to do with the information you're communicating. For example: "if you see this email, delete it but don't report it – we already know about it". In terms of the second, ensure that negative emotions such as fear or shame are not triggered. This is not conducive to durable experiences they can rely on.

Endsley, M. R. (2001, November). Designing for situation awareness in complex systems. In Proceedings of the Second International Workshop on symbiosis of humans, artifacts and environment (pp. 1-14).