This is a peer-reviewed, accepted author manuscript of the following research article: Renaud, K. (2022). D-F of cyber security. *Network Security*, *2022*(3). https://doi.org/10.12968/s1353-4858(22)70024-4

D-F 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***".

D: Debrief. When divers return from a dive, they reflect on: (1) what went right, (2) why did it go right? It is interesting to note that they do not initially focus on what went wrong even though lives can be lost when divers make mistakes. They focus on the positive behaviours that can be highlighted and emphasised for the benefit of others. When organisations experience a Phishing attack, there is often a myopic focus on the employees who fell for the attack. They are usually in the minority, but very few organisations look at the bigger picture: i.e., who saw the Phishing message and spotted it? What can we learn from what they did right so that we can better prepare those who were deceived?

Awareness raising efforts *must* calibrate their effectiveness, and continuously update their materials. Lessons learned in the aftermath of an attack offer us a golden opportunity to achieve this. Finally – be kind to those who are deceived. They feel bad already – it is never a good feeling knowing you've been hoodwinked.

E: Error: Errors can result from action (clicking on a link) or from inaction (not making a backup). James Reason wrote a seminal book about Human Error, which offers insights into human error. The first lesson is that error is unavoidable. The second is that no one ever eliminates their own propensity for making mistakes.

Humans make many errors, ranging from SLIPS (unintended actions – have you ever misplaced your keys?) to LAPSES (forgetting, which Atul Gawande wrote an amazing book about titled "The Checklist Manifesto") to MISTAKES (thinking you're doing something correctly, but getting it wrong) to VIOLATIONS (breaking a rule you weren't aware of) to SITUATIONAL ERRORS (wanting to do something but being unable to, perhaps due to fatigue or illness).

All of these are genuine errors – not driven by malice. It is thus unjust to punish the mistake maker. Remember, anyone and everyone makes mistakes – it could happen to line managers too.

The final category: RECKLESSNESS, is different. Here, the perpetrator knows exactly what they are doing and decide to break the rules and do it anyway. However, genuine errors are likely to dwarf these kinds of behaviours, and we ought not to attribute all errors to this category.

F: Fixation: programmers debugging their code are all too familiar with this. You keep trying to fix your code, but you only find the bugs when you realise that one

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

of your assumptions is unfounded. As soon as you come to that realisation, the lights go on. In cybersecurity, we sometimes focus on fixing one perceived vulnerability while neglecting to consider another. Mostly, people focus on human error, and don't really think about the possibility that hackers have compromised a system via an attack on the technology itself.

A good example is the WannaCry breach of 2017. The day the news broke, I saw someone write a news article saying something to the effect that somebody had clicked on a link in a Phishing message again. It was a knee jerk assumption because at that point no one knew how the computers were being compromised by the malware. Once the cyber security professionals started to check, they realised this was a very sophisticated zero day attack, which did not need any help from any human enabler. So: always challenge your assumptions.

Tune in next month as I continue my ramble down alphabet lane.