Moving from a Focus on Employee "Compliance" to Employee "Success" in the Cyber Security Domain

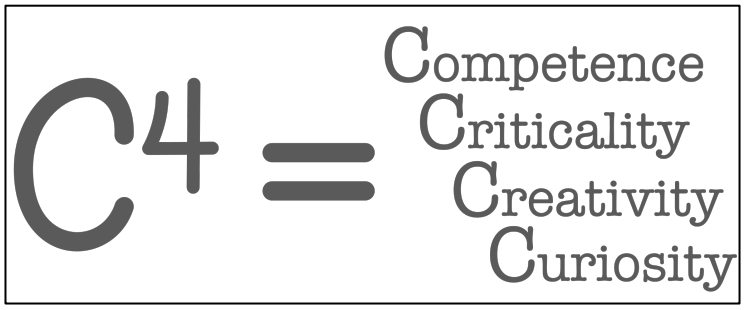
Karen Renaud[1,2], Stephen Flowerday[2], Marc Dupuis[3]
[1] University of Strathclyde, UK (karen.renaud@strath.ac.uk)
[2] Rhodes University, South Africa (s.flowerday@ru.ac.za)
[3] University of Washington, USA (marcjd@uw.edu)

Recently, the Wall Street Journal published an article about the use of fear in Cyber Security messaging [11]. The thrust of the author's argument was that the use of fear was unwise and counter-productive. Why is fear used in this context? Because the user of computer systems is often perceived to be the "weakest link" when it comes to cyber security. This is particularly true where the consequences of an employee's unwise action could be costly to the organisation [7].

Fear is merely the tool; compliance with security policy mandates is the aim, the underlying assumption being that fear is an effective mechanism to achieve compliance, and, transitively, more secure behaviours. This approach's flaws are two-fold. On the one hand, people dislike fear appeals [5], and many will respond negatively and not, as anticipated, by complying. But, even if they *do* comply, that is not necessarily a solution to the problem of insecure human behaviours. This is because this approach builds on yet another flawed assumption: that organisational policies are *sufficient* and *comprehensive*. This assumption is naïve for two reasons. The *first* is that cyber criminals innovate and change their tactics daily [9], while security policies take months to finalise. The *second* is that focusing on compliance attempts to turn employees into robotic rule followers. The underlying sentiment of "compliance drives" is that if employees would only follow all the mandated rules and follow processes, no security breaches would occur. While society cannot work without rules, this reliance on security policies is not appropriate in a domain as dynamic and fluid as cyber security [13].

Consider Phishing, the one exploit that is most successful in compromising organisations. In response to this threat, many organisations issue advice such as: "*Do not trust emails that come from people you do not know*" or "*examine embedded links in emails to make sure they are legitimate*" [4]. The first instruction might have been accurate a decade ago, but nowadays Phishers send emails that appear to come from regular correspondents, so this kind of rule does more harm than good [12]. For example, if a person is used to receiving emails from a regular correspondent and receives one with an attachment, he/she is likely to open the attachment without even considering that there is any need for caution. The fact that a Phisher is masquerading as a regular correspondent does not even enter the recipient's mind due to the familiarity of the correspondent and the accumulated trust between them. The attachment might well install malware as a consequence, because the person *followed the rule*. In the second place, cyber criminals are becoming so much sneakier at coming up with feasible-looking URLs that one almost has to be a computer scientist to identify the deception. The second instruction is often impossible for everyday users to carry out given the required expertise and how Phishers have become so adept at URL masking [8].

The proposal here is that we stop driving employees towards unthinking compliance, and rather replace the "one C" with "four C's". The idea is to help employees to become effective cogs in the security perimeter: the human firewall, as it were. When padlocks are manufactured, hardened steel is used. In the same way, we want employees to have a number of qualities that will give them the ability to recognise and resist attacks and thereby improve the security of their organisation's cyber domain, i.e., to "harden" them by enhancing and increasing their cyber security capabilities and deception-detection abilities.



What might hardening look like? In our opinion, we have to encourage everyone to develop the following qualities:

- **Competence**: People do not fall for Phishing messages because they *want* to. They "fall for" the deception; they are taken in sufficiently to click on the link or open the attachment. People need to develop a so-called "radar" – a sense of which emails are legitimate and which might be red herrings with malicious intent. Awareness is not enough: it is merely the first step – necessary but not sufficient. In addition to awareness, computer users also need to accumulate knowledge and build skills in this area. This takes time and support – there is no way to short-circuit this process. In the immortal words of Fred Brooks [2], there is no "silver bullet" when addressing complex issues.

  For example, one company that has taken this approach had assigned someone to be the "go-to" person for all cyber security queries. Anyone who got an email they were worried about could forward it to him. He was always respectful in his responses, whether their suspicions were grounded or not – thanking them for their vigilance. Moreover, he would send back an email confirming their suspicions by pointing out the red flags that they should look for next time, or reassuring them and highlighting the indicators of veracity they could rely on in the future. As the months went by, employees started developing a sixth sense about dodgy emails. The company then initiated a "catch of the month" award for employees who identified Phishing emails and alerted IT staff. The result was an end to successful Phishing attacks in that organisation. This approach is slow but effective and demonstrates a viable and effective alternative to a quick-fix fear-based approach.

- **Creativity:** At the moment, people are told to follow the rules and to do as they are told. On the one hand, this is demotivating. Jacob Bronowski [1] argues that people are not inherently lazy. He says that what appears to be laziness and indifference is a reaction to the fact that their job no longer fulfils them. This observation probably applies equally in the cyber security context. People are likel to feel constrained and hemmed in by an increasing number of rules and processes they are being required to comply with. They then become demotivated and, while this looks like laziness, it is actually a consequence of being treated like a robot or "a problem to be solved".

  Moreover, rules handed down from on high create a "we-they" situation where the powers that be lay down rules related to cyber security behaviours and the responsibility of the "others" is to obey the rules – not to innovate in defeating hackers. By taking this stance, organisations lose out – if employees are encouraged to come up with ways to defeat hackers, many more attacks would be foiled. When organisations promote these exchanges (i.e., leader-member exchanges), it increases positive change, novel ideas (i.e., creativity), and innovative behaviour [3].

  For example, in one organisation an employee witnessed a Phishing attempt. He first warned all his colleagues and then engaged with the Phishers and strung them along for days with ever more ridiculous requests for them to prove their integrity. He asked them to write him a poem, and then said it wasn't long enough, and so on. Eventually, they realised that he was playing a game with them and gave up. This employee was tremendously energised by this experience and felt proud to have foiled the Phishers' attempts to deceive his colleagues and cost his organisation money. Combining this with the previously-mentioned "catch of the month" award is likely to be particularly effective.

- **Curiosity:** should be encouraged, not extinguished, which is what rules attempt to do. What is needed is for people to be curious about cyber security, and organisations should nurture and satisfy employee curiosity in the cyber security domain. People love to hear stories, so stories can be used to excite interest.

For example, an acquaintance of one of the authors received an email saying that RyanAir was giving away free flights, if only they clicked on the link. Upon consulting one of the authors, a subsequent discussion about whether RyanAir had ever been in the habit of giving anything away led to a lightbulb moment. It raised awareness, which will help sharpen his judgment for future attacks. For some reason, people love to hear this story, probably because of the wry humour embedded in it and because it delivers a message about that particular Phishing message in a palatable way – not using fear.

Encouraging employees to tell their stories engenders a healthy curiosity about all things cyber and keeps it at the forefront of employees' minds. This will gradually upskill the employees and make it less likely that they will fall for Phishing messages. While the person in this story was aided by their curiosity, others were not as fortunate and fell victim to this Phishing campaign [14].

- **Criticality:** This is the final skill, which completes the circle. Say someone gets an email from a line manager, including an instruction to transfer money to a specific account. The rules would say: check that the email comes from the expected email address (the line manager), check that there are no links or attachments, check that the way the email is written aligns with the way it is usually written. If the employee follows these guidelines, the money is likely to be transferred. After all, realism in these factors is often what makes a Phishing email successful [6].

  In contrast, if the employee has been permitted and trained to be critical (and her curiosity has been kindled), the idea that the line manager's email account might have been breached might lead to a suspicion that the email might have come from a hacker. If the employee has had their critical faculties honed and encouraged, they might call the line manager to confirm the transfer. This will foil the Phisher, but if the employee has been trained to be a rule follower, the Phisher may succeed, pocket the money and leave the organisation with a vastly reduced bank balance. The employee, in this case, has dutifully followed all the rules, and they have proved insufficient.

What we suggest is that we move from “Compliant Charlie” to “Successful Sam”. Whereas Charlie follows the rules, becomes demotivated, and sees cyber security as a chore and an obstacle, Sam has become part of the secure perimeter of the organization. Sam is creative and curious, and has become competent and critical with the support of his employer. While a Phisher might still be able to get past Sam, it is a far more formidable prospect. David Marquet [10] urges us to change rule followers into leaders to improve employee morale and organisational outcomes. The four C's is calculated to achieve this. The ultimate goal is to strengthen the human firewall so as to fortify this first and crucial line of defence. As a side effect, we will also get happier and more fulfilled employees who do not feel side-lined, stupid or unimportant when it comes to defeating the hordes of invisible and pesky cyber criminals that seek to compromise their organisations.

[1] Bronowski, Jacob (2008). *The origins of knowledge and imagination*. Yale University Press.

[2] Brooks Jr, F. P. (1995). *The mythical man-month: Essays on software engineering*. Pearson Education.

[3] Carnevale, J. B., Huang, L., Crede, M., Harms, P., & Uhl-Bien, M. (2017). Leading to stimulate employees' ideas: A quantitative review of leader–member exchange, employee voice, creativity, and innovative behavior. *Applied Psychology*, 66(4), 517-552.

[4] CrimeStoppers. (2017). How to tell if an e-mail is genuine or a phishing email. https://crimestoppers-uk.org/campaigns-media/blog/2017/jun/how-to-tell-if-an-e-mail-is-genuine-or-a-phishing-email

[5] Dupuis, M., & Renaud, K. (2020). Scoping the ethical principles of cybersecurity fear appeals. *Ethics and Information Technology*. https://doi.org/10.1007/s10676-020-09560-0

[6] Dupuis, M. J., & Smith, S. (2020, October). Clickthrough Testing for Real-World Phishing Simulations. In *Proceedings of the 21st Annual Conference on Information Technology Education* (pp. 347-347).

[7] Ifinedo, Princely (2018). Roles of organizational climate, social bonds, and perceptions of security threats on IS security policy compliance intentions. *Information Resources Management Journal*, 31(1), 53-82.

[8] Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences*, 10(1), 1-41.

[9] Lee, L. (2019). Cybercrime has evolved: it's time cyber security did too. *Computer Fraud & Security*, 2019(6), 8-11.

[10] Marquet, David. (2015). *Turn The Ship Around!: A True Story of Turning Followers Into Leaders.* Penguin.

[11] Renaud, Karen. (2020) Why Companies Should Stop Scaring Employees About Cybersecurity Dec. *Wall Street Journal*.

[12] Vayansky, I., & Kumar, S. (2018). Phishing–challenges and solutions. *Computer Fraud & Security*, 2018(1), 15-20.

[13] Zimmermann, V., & Renaud, K. (2019). Moving from a "human-as-problem" to a "human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies,* 131, 169-187.

[14] Zurkus, K. (2018, August 31). Mobile Phishing Campaign Offered Free Flights. Infosecurity Magazine. https://www.infosecurity-magazine.com:443/news/mobile-phishing-campaign-offered/