Learning from the past ….

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

I've been reading an excellent book by Eleanor Herman, titled "The Royal Art of Poison". Now, you may be wondering why on earth I am telling you this, when this is a column about cyber security. I'll explain.

The author tells a number of stories about the use of poison in the middle ages, and the precautions wealthy people and royalty would take so that they would not be poisoned. They had tasters who would eat from their plates and others who would imbibe wine from their goblets. Eleanor Herman tells about people paying a fortune for unicorn horns, which could apparently neutralise poison. Some Kings thought they could be poisoned by the clothing they wore, or the seats of their commodes. If they did fall ill, it seems that the first thought was that they had been poisoned. Pity the poor chefs who worked in royal households who were tortured and executed for attempting to poison their masters when they were actually suffering from gastritis, malaria or a swollen prostate. It must have been a fearful existence for everyone.

The problem is that these wealthy people focused on external threats – from those within and outside their own households. At the same time, they used mercury-based creams to whiten their skin, took arsenic for their ailments and added lead to drinks to sweeten them. Of course, they didn't know that these were poisonous, but exhumations carried out in the 21st century have found extremely high levels of mercury, lead or arsenic, much of it self-administered. They looked outward and the threat came from what they themselves were doing.

There are some lessons we can apply in the cyber security context:

(1) We often focus on the nameless outsider – the cyber criminal or scammer. But, organisations don't think about the things they do that poison the well, as it were. There are some basic housekeeping tasks that should be taken. For example, making regular backups provides resilience. It's as essential that that yearly boiler service. Backups must be air-gapped, otherwise ransomware might encrypt them as well[1].

Companies should implement two-factor authentication. Google reported how this one thing halted the effectiveness of Phishing attacks against their organisation[2].

(2) Organisations often blame their own employees when a cyber event occurs, even when it is their own processes or systems that are at fault. Consider

[1] https://www.planbconsulting.co.uk/blog/case-study-dundee-and-angus-colleges-cyber-attack-communications-review

[2] https://www.techradar.com/news/google-reveals-how-it-has-stopped-phishing-attacks-for-good

the case of Patricia Reilly[3] who fell for a Phishing attack and transferred £193,250 to a Phisher's account. The company fired her and then attempted to sue her for the money that the bank did not refund. The judge found for the defendant because "*there was no evidence training was available at the time to address this type of fraud*"[4]. He also said that "*the fraudster is the real culprit whoever he or she (or possibly they) may be*".

(3) Organisations carry out Phish simulations on their own employees. This communicates a lack of trust in these employees, and such organisations are repaid by a lack of trust in return. This is indeed a pity because everyone needs to work together in organisations if we're going to have a chance of improving cyber security. Treating your own staff with suspicion is not the way to achieve this.

"If we don't learn history, are doomed to repeat it". Philosopher George Santayana

[3] https://www.bbc.com/news/uk-scotland-glasgow-west-47135686

[4] https://www.peoplemanagement.co.uk/news/articles/credit-controller-does-not-have-to-repay-employer-108000-lost-in-email-scam