Prescott Kowalski

Professor Umphlet

3May25

Analytical Paper

Introduction

As many know, experts such as, Hans Jonas, prefer that we would take a short arm approach to attacking change in cybersecurity. Personally, I believe, society should be attacking at the development of cyber-policy and infrastructure with the sense that it will be constantly evolving. A short arm being like giving a dog a treat. You know well ahead of time that there is so much left to be discovered in this field, especially with the adaption of AI. Policies must be extremely adaptable, with infrastructure ready to take on and recover from any upcoming threats. Education must also be this way, as the new generations must be ready for the unpredictable future. There are so many unknown factors about these, as well as evolving is highly likely. Adaptation also improves the integrity of these systems, a staple in the CIA Triad.

Advances and Threats

To begin, Hans Jonas exclaims we are mere mortals compared to technology “Not even within its artificial space, with all the freedom it gives to man's determination of self, can the arbitrary ever supersede the basic terms of his being.” (Jonas P 37) Claiming technology supersedes us in many ways, it should be attacked accordingly. Following a short arm approach, gives us humans an advantage at understanding technology. As it will always get better, year by year, we must always be on top of it. As we are mere mortals not capable of eternal life, unlike computers which are.

To give a dog a bone, hospitals have also been attacked by ransomware, leading to a violation of HIPAA and more. “Hospitals consolidating into large multistate health systems face increased risk of data breaches and ransomware attacks, according to one study… And while cybersecurity regulations can quickly become outdated, they can at least make it clear that if health systems fail to implement basic protections there “should be consequences for that,” Jim Bagian, a former director of the National Center for Patient Safety at the Veterans Health Administration, told Michigan Public’s Stateside” (Pradhan P 32-33) Improving the integrity of cybersecurity infrastructure will help prevent these issues as well as protect the rights of the public. The last thing you want are your own private health records being held ransom because of a system lacking integrity. This must be regulated and others should be held responsible for their lack of well-being.

The Dog Treat

Given how, patient data is extremely sensitive, and the consequences of a breach are very severe, though cybersecurity measures integrity should be protected. As the second letter of the CIA triad, it is vital to be recognized. Leading to potential breaches, a lack of cybersecurity infrastructure can lead to patients’ rights being violated at hospitals, fines to the hospital and other places as well as operational discrepancies. Modernizing these cybersecurity infrastructures with a short arm approach (giving a dog a bone) by slowly attacking the infrastructure for solutions, will greatly help for the future of technology.

With fines also being a powerful incentive, it is vital to make sure cybersecurity infrastructure has great integrity as well. This is where giving the dog treat comes in, with a slow, steady and adaptable approach to cybersecurity infrastructure, integrity will strengthen. Similar to a dog slowly learning a new trick from a reward, you can slowly trust that your data will not be messed with, this also will lead to confidentiality and availability of your product increasing. A short arm is what gets you there, the main issue being the unpredictability of the threats to infrastructure etc. Comparing this to the unpredictability of a learning dog, it is always worth the risk. You always want a constantly learning infrastructure, the more threats it is aware of taking care of and the more it can handle, the less likely violations will happen like HIPAA.

Conclusion

Treating cybersecurity like a dog, by using Jonas' short arm approach, is crucial for the CIA Triad. With integrity being improved by watching it intensely, slowly but surely making progress towards the goal, and understanding that we as humans are mere mortals as said by Jonas, cybersecurity infrastructure can flourish. This will help prevent HIPAA violations, protect against ransomware, higher availability of the product, improve confidentiality, and ensure the durability of the infrastructure. With the main issue with the cybersecurity infrastructure being like a learning puppy, you can expect hiccups from time to time, but with proper addressing this will be no big issue. Tying back to the CIA Triad, everything must be perfectly balanced. Without this balance, like a puppy not being trained properly, other aspects of the triad can falter, like the availability of the infrastructure from downtime or the confidentiality being messed with from a lack of protection.

References

- Pradhan, Rachana, and Kate Wells. “Cyberattack Led to Harrowing Lapses at Ascension Hospitals, Clinicians Say.” *NPR*, NPR, 19 June 2024, www.npr.org/2024/06/19/nx-s1-5010219/ascension-hospital-ransomware-attack-care-lapses.
- JONAS, HANS. “TECHNOLOGY AND RESPONSIBILITY: REFLECTIONS ON THE NEW TASKS OF ETHICS.” *Social Research*, vol. 40, no. 1, 1973, pp. 31–54. *JSTOR*, http://www.jstor.org/stable/40970125. Accessed 28 Apr. 2025.
-