Practitioner-Scholar Research Conference

2021 Abstract 4 18-19 June

FEDERICO GIOVANNETTI

ARE INFORMATION SECURITY AWARENESS PROGRAMS USING THE RIGHT APPROACH?[1]

Keywords: *security awareness, human risk, behavior, psychology, sociology*

Information security departments, typically led by a Chief Information Security Officer (CISO), continue to be challenged and frustrated by the lack of employee compliance with established security policies. At times, it seems as though some employees try to outright bypass information security safeguards in favor of accelerating their business objectives, causing tremendous frustration for security practitioners. On the other hand, as security practitioners assume a policy enforcement role, the rest of the company increasingly sees them as an obstacle to achieving their main objectives. This creates unproductive reinforcing behaviors where the two parties increasingly grow further apart, making it very difficult to achieve the goals related to improving the information security posture of the organization. Ultimately, the goal of the CISO department is to protect the confidentiality, integrity, and availability of the information assets of the organization. For this reason, a program that reduces the risks associated with employees' lack of compliance should be a welcome addition to their tool chest.

It is not uncommon to find studies, as well as collective opinion, claiming that employees are the largest source of security incidents. In addressing this problem, practitioners and scholars have focused on analyzing employee behaviors. Several individual factors have been studied, such as carelessness, lack of knowledge, and employee perceptions (of cost, vulnerability and/or sanctions), among others. It follows that devised interventions have focused on how to change those behaviors using techniques such as persuasion and influencing.

A number of vendors in the industry have recently been quite successful providing products and services designed to solve this problem. The product they provide is usually known as "Security Awareness Training" (SAT) and it consists of cleverly designed training materials including engaging videos and gamification, coupled with simulators that test the employees' ability to react to unexpected cyber-attacks. The "human risk" problem has also been recognized by the security practices auditing apparatus. Established audit frameworks such as PCI-DSS, SOC 2 and HIPAA, all contain requirements for companies to include SAT in their practices. In addition, many organizations, especially in the finance,

government, and health sectors, require technology providers to implement SAT before they can do business with them.

Is Security Awareness Training the right approach to deal with this problem? Some critics have said that it has become another mandatory compliance requirement that is easy to check by employees and soon forget about. Others claim that the current state of the art only focuses on social engineering attacks such as phishing, leaving other non-compliance behavior such as weak passwords or software patching outside. Arguably, the current offer can be improved to address these shortcomings. However, the premise remains the same, namely trying to influence and persuade individuals to change certain behaviors, suggesting that the problem is related to the individual as opposed to the organization as a whole.

Does the Information Security industry conceptualize humans solely from a psychology or cognitive behavior angle? An affirmative answer certainly seems to match the current interventions directed at individuals (mostly SAT). If so, should this approach be replaced or at least complemented with one that draws from sociology/anthropology and studies group dynamics such as working environment, business pressures, management demands, etc.?