Yengkong Sayaovong

1/22/2023

Lab 4:

The Human Threat

Summary: The article discusses about business around the world are adopting the military's cyber security practices. The article talks about making it a priority to minimize the chance of having human errors as the most important thing. The article also mentions that if people would update their security systems on a regular basis, it would greatly reduce the issue of human error. In the article, Admiral Hyman Rickover discusses six principles that the U.S. Navy does in order to minimize human error. Although it was the U.S. Navy who came up with these principles, companies throughout the world can also adopt and use these principles as a guide in order to reduce human error in their company.

Analysis: The article by Winnefeld, Kirchoff, and Upton argues that the biggest issue within the world of cyber security is human error. An example of human error in the article is administrators installing malware because they thought it was a system update. This claim are strongly supported within the text through the constant comparison of company cybersecurity policies and those of the U.S. military. The article get these comparisons with the idea that the U.S. military has the most secure policies when dealing with cyber security attacks. The article demonstrates the security measures many companies have in place. One of the main issues that the article presents is that when considering security policies, many chief executives "are not moving fast enough because this task can be massive an expensive" (Winnefeld 2015). This appears to be an ongoing issue for corporations. According to Ariel Levite, "the private sector is struggling to contend with the growing scope, scale, and complexity of cyber risks to corporations" (Levite, Kannry & Hoffman 2018). However, the private sector has become more aware of the severe consequences that cyber-attacks can have, and larger entities have begun to face these issues head on. Although the private sector has increased its awareness of cybersecurity, accountability, and initiative towards improving security continues to be lacking. In a modern world where technology continues to advance, corporate security policies must be able to keep up, and they will not update on their own. Recently, the Defense Information Systems Agency has updated its cyber defense strategy for the next three years. However, Navy Vice Adm. Nancy Norton states that "implementation had to be

accelerated at a very rapid pace" (Williams 2020). Regardless of the major technological advancements that are made in the world of cybersecurity, no progress in security will be made unless Chief Executives and administrators take the initiative to acknowledge the importance of cybersecurity and make it a priority to always have the most effective and current policies.

Citations:

David M. Upton Sadie Creese, Fick, N., & David M. Upton and Sadie Creese. (2016, September 09). Cybersecurity's human factor: Lessons from the Pentagon. Retrieved January 23, 2023, from https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon