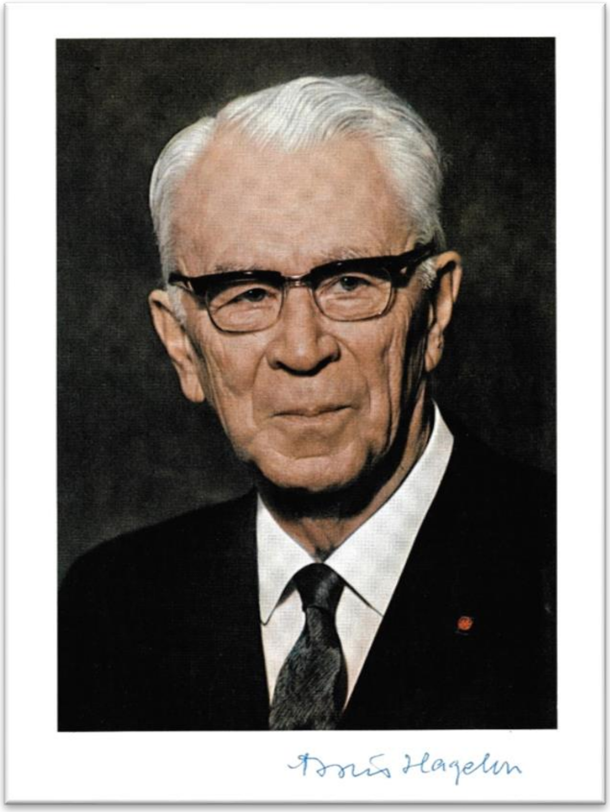
The Old Rule --- A System is Only as Good as its User October 29



HISTORIC QUOTE: “The old rule is still true: the quality of a machine depends largely on its user.”

This was the last line by Boris Hagelin in his 1981 publication entitled “The Story of the Hagelin Cryptos.” It reminds us that when it comes to core principles behind communications security, information assurance, or cybersecurity, some things never change.

Born in Russian Azerbaijan in 1892 to Swedish parents, Boris Hagelin grew up in a family with strong ties to business, especially with the Nobel family and its business interests in Russia. However, after the Bolshevik Revolution broke out in 1917, the Nobels and the Hagelins moved their interests back to the safety and security of Sweden. By this point Boris Hagelin had earned a degree in mechanical engineering and was working for Nobel.

In the early 1920s, the Nobels began financing a small company in Sweden called A.B. Cryptograph, which manufactured cipher machines based on designs of its founder, Arvid G. Damm. Hagelin eventually became manager of this firm when it was reorganized into A.B. Cryptoteknik after the death of Damm in 1927.

During the 1930s, Hagelin’s rebranding and re-engineering of the products struck the right cord at the right time with the U.S. Army and its chief cryptologist, William Friedman. In *The Codebreakers*, author David Kahn states that Hagelin was the first man to become a millionaire from cryptology, primarily from the sale of the M-209 model cipher machine which was used by the U.S. Army for its midlevel communications during and after World War II. After the war, Hagelin's firm grew even bigger as the trademark "Hagelin Cryptos" became well known internationally (to those in the secret communications business) and the firm moved to Switzerland, rebranding itself again as Crypto AG.

In "The Story of the Hagelin Cryptos," Hagelin described the history of the cryptologic business as well as the details of some of his most famous models and prototypes. In his closing observations, he acknowledged how the use of computers was becoming routine in cryptanalysis, but warned that good communications security is only as good as the humans behind the system. He stated, "For cryptanalysis it is mandatory to know the characteristics of the machine. In addition the cryptanalyst gets considerable help from poor operational practices of the machine. Human errors can simply not be eliminated. On the other hand the cryptanalyst today still has the chance of success through his own intuition as he depends on the 'probable word', i.e., on stereotyped, often used expressions. Direct betrayal or unintentional indiscretion naturally do not belong to the technique of cryptanalysis. This art depends mainly on statistical methods, which allows the recognition of repetitions of chosen machine settings which arise through overlaps of keying periods. For this reason secure cipher communication requires not only good equipment but also cryptologically trained personnel to prepare the operating instructions for the machine, and very trustworthy, well trained operators who strictly observe these instructions."

Sources: "The Story of the Hagelin Cryptos" by Boris Ceasar Wilhelm Hagein (1981); *The Codebreakers: The Story of Secret Writing* by Davis Kahn (1967)