Cybersecurity and the "Return on Negligence"

by Gary C. Kessler, Ph.D., CISSP

One decade later:

It was a question one business owner asked me a few weeks ago: "Is your company only worth $10,000?"

More often than not, we are reminded of the importance of cybersecurity to our enterprises. If the question of whether the protection and mitigation of the threats to our organizations are worth the investment into our cybersecurity is asked, the answer is generally yes. Is your company's cybersecurity worth $10,000?

We are asking the wrong question. The real question is how much money, time, and resources are we willing to allocate to secure our cyber assets?

The logical remedy for PIP threat is in question. A client recently approached me about a potential new opportunity. "Is it worth it?" the client asked. "The potential for a loss is significant, but the impact to our business is small. Do you think this is a worthy expenditure?"

To address whether the potential loss is worth the investment, the client was asked to answer five basic questions:

1. What is the likelihood of a vulnerability being exploited? What is the potential impact of an event? Note that you don't have to estimate how often we expect such an exploit to actually happen. In more formal terms, the Annualized Loss Expectancy (ALE) is the product of the Single Loss Expectancy (SLE) times the Annual Rate of Occurrence (ARO). And compare the cost of these controls to the new ALE. If the defense cost is greater than the new ALE, the investment is not cost-effective.

2. What are the primary threats to your business and their likelihood? Is the potential impact on a shipping company or port if a cyberattack causes death, a very real possibility in the maritime industry, sufficiently compelling? And if these consequences are not sufficiently compelling, consider that the loss of intellectual property (IPI) could also have severe ramifications. The U.S. Executive Order 13636 for Critical Infrastructure Designates Maritime and Port Security as having the potential to be a national emergency, and require federal action. Gary C. Kessler, Ph.D., CISSP is a professor of cybersecurity at Embry-Riddle Aeronautical University.

Gary C. Kessler, Ph.D., CISSP is a professor of cybersecurity at Embry-Riddle Aeronautical University and educator. More information can be found at https://garykessler.net.

The opinions expressed herein are the author's and not necessarily those of The Maritime Executive.

© Copyright 2018 The Maritime Executive, LLC. All rights reserved.