Topic: The State of Industrial Cybersecurity.

1. What are the major threats and risks in industrial cyber systems?
2. What can we do to mitigate the risks in engineering cyber systems?

Name: Julia Painter

Date: February 24, 2019

The growth of cyber systems in the industrial sector has lead to a growth in the types of threats. The increase in the use of cyber systems permits an increase in the potential for weaknesses or vulnerabilities. Because of mistaken perceptions of the risks associated with cyber systems, industries can leave themselves completely at risk for attacks on their cyber systems. False or misplaced confidence is especially fatal when it comes to the security of an industry's cyber systems. For this reason, it is important that one be aware of the reality of threats toward cyber systems and the types of measures that must be done in order to stave off attacks.

According to a research study conducted by both Kaspersky Lab and Business Advantage on industrial cyber security professionals, the perception said professionals have regarding cyber security threats tends to differ from the actual threat level. This is to say that a tendency to be overly concerned with types of threats that are not as prevalent and underestimate the likelihood of threat that have a greater chance of occurring appears to exist (Business Advantage, 2017). These results of this research identify conventional malware and virus outbreaks, targeted attacks such as advanced persistent threats, and human error as the three leading causes for concern within organizations (Business Advantage, 2017). This is particularly interesting because these were not conveyed as being the three greatest reasons for concern within organizations. Therefore, this lack of awareness of the true dangers organizations should be focused on defending against poses a challenge to achieving a secure cyber security system.

With all of the potential threats and dangers that a cyber security system could potentially fall prey to, it is important that efforts be made toward specifically defending against any attacks. Before any effective measures can be made to prevent cyber security attacks, it is important that companies make themselves properly aware of what their individual weaknesses and potentially exploitable vulnerabilities are. Some companies may be more adept to handle certain types of attacks than others. It is also true that some organizations may be more likely to be victimized by a certain type of attack due to the nature of the business that said organization handles. Therefore, it is important that each industry implementing cyber security networks determines its own individual weaknesses. It is also recommended that cyber security specialists and staff be hired to handle the determining and protecting the company based on its specific security needs (Business Advantage, 2017).

Industrial cyber security threats are not just an issue for one specific nation; it is a worldwide problem. Unlike some problems, the potential for cyber security threats is far from temporary. It is unlikely that protecting against cyber threats will become an obsolete task any time soon. As technology continues expanding, the potential for new and ever-changing threats will grow as well. It is for this reason that those relying on cyber security systems become and remain aware of the potential dangers to said system so that they may be prevented as effectively as possible.

References:

Business Advantage. (2017). The state of industrial cybersecurity 2017 [PDF File]. Retrieved from https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf