ABB Cyber Security Risk Reduction Roadmap

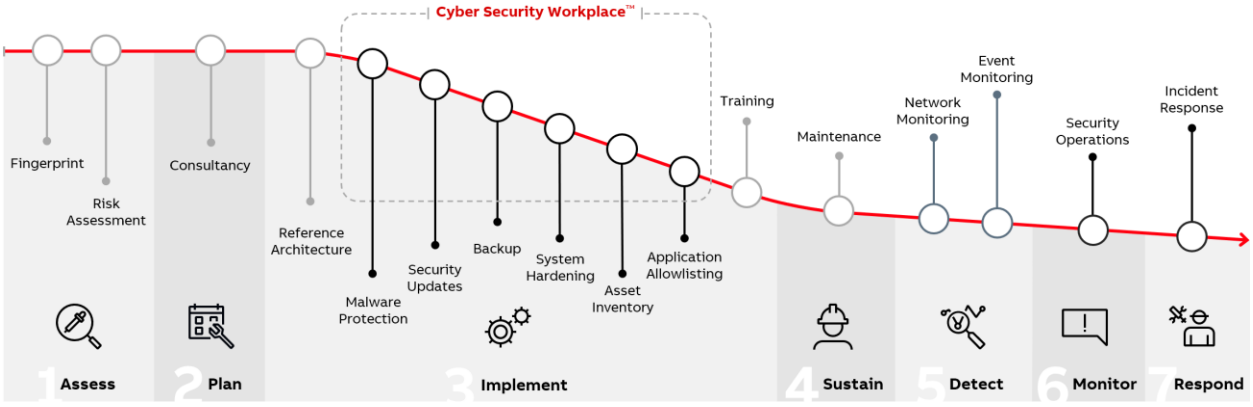
The Industrial Cyber Security Journey

Industrial cyber security is all about managing and reducing risk. Risk is a function of the likelihood of something happening and the consequence of that something happening. By this definition, one can approach risk reduction in many ways as long as the security measure reduces the likelihood or consequence. Security controls that address the likelihood of a cyber incident are, for instance, hardening, applying security updates, and monitoring for malicious activity. Backups and training are the main mechanisms to reduce the consequences of a cyber incident.

Which security controls and actions should one apply before the others to achieve the most reduction?

To support industrial cyber security, ABB has created the Risk Reduction Roadmap. The roadmap proposes which security steps one should take and in which order. The roadmap also indicates the risk reduction one item is likely to provide.

Figure: ABB's Industrial Cyber Security Risk Reduction Roadmap.



The risk reduction roadmap (as shown above) should be read from left to right and is divided into seven steps.

1. Assess: ABB recommends beginning with assessing the system. A quick fingerprint or a comprehensive risk assessment can do this. The assessment step is essential even though it doesn't directly reduce the risk, as depicted by the flat red line.
2. Plan: Planning and documenting what one wants to achieve is essential. This plan can then be consulted during the journey. As with any plan, it must be revised and updated over time. Like the assessment phase, the plan doesn't reduce any risk.
3. Implement: This is where security controls are implemented, and the risk reduction starts.
    a. Reference Architecture: A well-designed network is a foundation for adding all other security. ABB's ICS Cyber Security Reference Architecture outlines our industrial cyber security experts' recommendations.
    b. Malware Protection: Malware (aka viruses) is still a significant risk to any computer system. Implementing malware protection is one of the first things one should do.

c. Security Updates: Any software-based system has vulnerabilities that malicious attackers use to accomplish their objectives. Applying security updates to close these vulnerabilities is among the top priorities to reduce risk.

d. Backup: Once an attacker is successful, the only thing you can do to reduce the risk (consequence) is to get the system back up. A good backup is often the primary tool to accomplish this.

e. Hardening: An industrial system should be hardened where settings, services, and applications are reviewed, and anything not needed for production must be removed or disabled.

f. Asset Inventory: Knowing what you have (both hardware and software) enables you to address obsolete components proactively before they are compromised. It is also a tool that helps you quickly identify if you are vulnerable to newly reported threats.

g. Allowlisting: This security control is compelling but, unfortunately, not the most straightforward one to manage. It reduces the risk by preventing anything that is not explicitly allowed to be executed. In theory, a malicious application must not be allowed to run and, therefore, cannot infect the system.

h. ABB Ability™ Cyber Security Workplace: This ABB-developed application simplifies the management of security controls by providing a unified interface.

i. Training: One often disregarded security control is training. Having everyone ever in contact with the production system or any part thereof trained is vital. If everyone is vigilant about cyber security and trained to detect malicious behavior and methods, it significantly reduces the risk.

4. Sustain: This step is crucial as any prior investment loses its effectiveness if not maintained.
5. Detect: The following tool to reduce risk is to deploy technology to detect malicious activity. One can select event or network monitoring. For maximum risk reduction, one should apply both as each operates differently and each augments the other.
6. Monitor: The detection step is wasted unless someone monitors the alerts the detection tools provide. A common way to address monitoring is to deploy a security operation center (SOC) where skilled personnel constantly monitor the system for malicious activity.
7. Respond: If something happens, one must be able to respond to the threat or attack.

The risk reduction roadmap is ABB's recommendation on how an industrial system operator could approach cyber security for the most significant impact. However, the steps or the order in which they appear on the roadmap is only a recommendation. Sometimes, a valid justification exists to implement items in a different order, add security controls, or omit some.

—

For more information, please contact:

Patrik Boo
Email: patrik.boo@us.abb.com