MANGAN INC. Cybersecurity

REAL Matters

Protecting Your OT Assets and Infrastructure

ICSSbD™ Industrial Control System Secure by Design

Volume 1, Advisory #10 – August 2022

REAL Matters advisories are published to communicate cybersecurity threats and risks within the Operational Technology (OT) environment and where Critical Infrastructure vulnerabilities are identified. The purpose of this newsletter is to inform, propose suggested approaches to mitigate the risk as well as provide feedback on how Mangan Cybersecurity is approaching the issue(s) addressed.

Advisory Information

At A Glance

Issue Date:	August 8, 2022
Summary:	Zero Trust is “Gonna Take a Revolution”. This REAL Matters talks about embracing a Zero Trust mindset to meet and exceed expectations.
Systems Impacted:	All Confidential Information, Project Design Documentation, Project Support Documents
Importance:	Very High

Details

The basis of the Zero Trust Security Model is the belief that threats exist not only outside of the network but INSIDE the network boundaries as well. It is imperative to continually question the implied belief that users are who they claim to be, and that the computers and systems on the network are authentic and that the information stored on those systems are safe, secure, and protected from compromise and malicious attack. Adopting the Zero Trust mindset requires both parties execute with the following at the forefront:

- ***Do not trust and always verify*** your cyber assets and your cyber partners. Assume malicious intent.
- ***Consider confidential and restricted information*** placed in the hands of others (e.g., service providers) and expect an established information security posture. This means having a plan to distribute this information securely and based on need-to-know. This also means having a plan to cyber-shred the data when need-to-know expires.
- ***Expect monitoring as well as rapid damage control and recovery*** by the service provider if managed information is altered, damaged, or attacked.

Actions and/or Recommendations

Designs and solutions must consider and include the Zero Trust Security Model. Whether this requires encrypting client sensitive information, managing vendor purchase orders, or restricting access to detailed design documents and implementation guides, all systems, projects, and control systems will use and produce confidential client information; this is not if it occurs but rather an assurance that it will! Therefore:

- Identify at the project process outset the Zero Trust dependent critical Data, Assets, Applications and Services also known as the project ZT DASS (pronounced zee tee dass (*rhymes with class*))
- Plan to protect the ZT DASS and secure and demand secure paths to that data.
- Create security policies to control view, use and distribution of the ZT DASS. Understand, email is not a secure channel to send information.
- Use traffic logs and be made aware when any sensitive information is subject to suspicious activity.
- Adopt the Zero Trust mindset by Evolution or by Revolution.

About Mangan Inc.

Mangan Inc. is a nationally-recognized Specialty Engineering, Automation, and Integration company, providing a full-range of services to the Oil & Gas, Refining, Pipeline, Chemicals, and Life Sciences Industries. Established in Long Beach, California in 1990, Mangan’s multiple office locations include sites in California, Georgia, New Hampshire, North Carolina, Texas, and Louisiana. Mangan’s 350+ employee-owners bring expertise, innovation, and safety as their core mission to some of the largest companies in the world.