Society for Maintenance & Reliability Professionals

SMRP Policy Recommendation: Promote, develop, and implement a strategy for evaluating the impact of IoT devices and systems as it pertains to cybersecurity and infrastructure for small to large-sized business.

With advances in cyberphysical and cyberinformation systems (known as the Internet of Things (IoT)), unparalleled opportunities for improved monitoring, operations, and reliability of systems have been made readily available to all aspects of personal, public, private, and commercial entities. However, through rapid advancement and deployment, significant cybersecurity issues and infrastructure vulnerabilities have arisen as organizations do not necessarily understand the impact of a full threat.

A majority of IoT systems are implemented as monitoring systems and related maintenance systems within organizations and via third party maintenance organizations. These have the possibility of producing weaknesses in information security (cyberinformation), which may include critical operational and financial information, and access to controls, which may include the ability to effect systems and infrastructure (cyberphysical). Specialized search engines, such as Shodan.io, can easily identify internet connected systems, including maintenance systems, which provide support for internet security professionals who are verifying the accessibility of their systems, as well as cybercriminals who are searching for vulnerable systems. A great many applications for all operating systems, such as those for supervisory control and data acquisition (SCADA) systems, are freely available that can access systems for remote monitoring and operation.

Cybersecurity Case Study: Target, 2013

On November 15, 2013, a complex cyberattack was conducted on Target stores through credentials obtained from a third party HVAC service company. Once cybercriminals obtained access to a beachhead in the HVAC service company's contractor billing, contract submission and project management system, they were then able to use information provided via the portal to access Target's credit card terminals. From November 27 to December 18, 2013, cybercriminals gained access to over 110 million consumer credit cards via Target's email system.

At the present time, there is little to no understanding of the impact of cybersecurity issues resulting from third party vendors or on small to medium-sized manufacturing facilities.

It is SMRP's position that while an emphasis on larger organizations is important for a last line of defense, preventing cyberattacks on small to medium-sized organizations, and those that provide services to large-sized organizations and critical infrastructure should be the main focus. It is SMRP's belief that an understanding of threats through IoT devices, contractors and subcontractors, regardless of size, and the development of cyberdefense processes will further reduce the risk to the economy and infrastructure of the United States and its allies.

SMRP recommends research into the potential threat through the first line of defense and the inter-connectivity between companies, vendors, contractors and subcontractors with an overall goal to establish a cyberdefense strategy. This includes the evaluation of cyberinformation, cyberphysical systems and best practice methods to prevent infiltration and damage to the front-line organizations. In essence, this will have an additional impact on improving security for small to medium-sized businesses while reducing the number of attacks on larger organizations. Because current business models for larger organizations include contracting services through smaller companies, this presents an inherent problem as smaller firms are more prone to

cyberattacks and can inadvertently exploit sensitive information from larger organizations. As a result, SMRP also recommends including the development of a vetting process and identification of tested and secure IoT devices and systems.

SMRP Impact

SMRP consists of maintenance, reliability and physical asset management professionals involved in all aspects of industry, utilities, government, and support organizations. SMRP members are uniquely positioned to identify the impact of cybersecurity implementation on the reliability of the infrastructure, generation, and commercial / industrial end users. SMRP has developed enhanced tools that provide best practice metrics, benchmarking and reference materials for maintenance and reliability improvement. SMRP's participation in global collaboration related to physical asset management, which is a framework for managing complex systems, includes recognized certifications from reliability programs to asset management, such as the ANSI-certified Certified Maintenance and Reliability Professional (CMRP) as well as the Certified Maintenance and Reliability Technician (CMRT) and internationally organized Certified Asset Management Assessor (CAMA).

SMRP Commitment

SMRP is committed to assisting:

- In the development of a study on cybersecurity issues within SMRP's membership.
- An understanding of the cyberinformation and cyberphyiscal systems that are in development and / or needed for performance of reliability and maintenance functions including monitoring of equipment.
- The understanding of how big data improves cybersecurity and its impact on small to medium-sized manufacturing facilities.
- Development and training on the importance of cybersecurity for small to medium-sized manufacturing facilities and third party vendors.
- Assisting in the development of a process for evaluating the security impact of IoT devices and systems.

SMRP Recommends

SMRP makes the following recommendations:

- SMRP supports a federal study on cybersecurity issues related to small to large-sized businesses and related infrastructure and third party support vendors including reliability and maintenance contractors and IoT suppliers;
- SMRP supports the development of training and awareness programs for general industry, third party suppliers, IoT providers, and other stakeholders in relation to the threats and impacts of cybersecurity issues and vulnerabilities;
- SMRP supports the development of a process, or processes, to vet IoT devices and related systems and software for potential vulnerabilities;
- SMRP supports the development of a process, or processes, to vet third party vendor cybersecurity and vulnerabilities.