FLUKE®
Reliability

Managing Cybersecurity Risk in Maintenance & Reliability

Best Practices Webinar Series

Speaker Bio

Matthew Hudon

CISO, Fluke Reliability

- 15+ years of experience in designing and implementing secure IT solutions
- Has helped dozens of companies and product team standup compliance and security programs for various standards (e.g., PCI-DSS, ISO, HIPPA, SOX)
- Has been leading cybersecurity for Fluke Reliability for the past two years

Speaker Bio

Frederic Baudart

Lead SME Manager, Fluke Reliability

- Lead SME Manager Specialist at Fluke Corporation for past 6 years
- 20+ years experience in field service, engineering work, PM and reliability
- Focusing on company's reliability and condition monitoring solutions, IIoT programs and product support
- Held various field services and technical positions responsible for:
    - Installation and Commissioning
    - Product Management
    - Territory Technical Sales
    - Senior Services Management Roles

POLL QUESTION No. 1

Is Cybersecurity an important factor when considering a M&R solution?

(Click only one answer)

- Mission Critical
- Somewhat Important
- Not Important
- Not Sure

FLUKE Reliability

Agenda

What is Cybersecurity?

Why Cybersecurity is Important in Maintenance and Reliability

Cybersecurity & IIoT “In Action”

- Government
- Healthcare
- Manufacturing

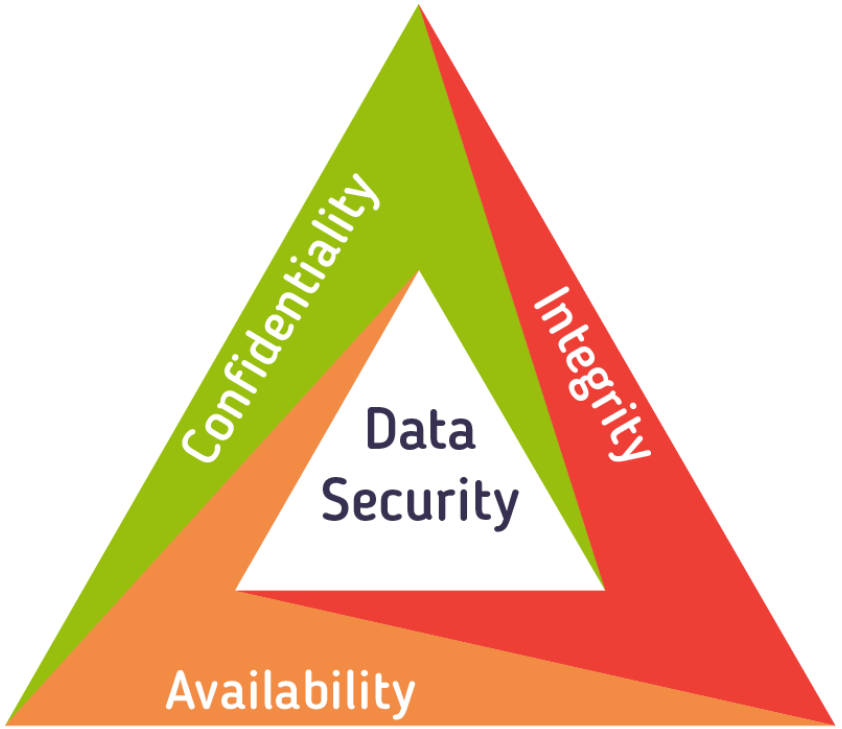
Q & A

FLUKE® Reliability

What is Cybersecurity?

CIA Triad

- **Confidentiality**
  - Ensuring that only people with permission have access to your data and information
- **Integrity**
  - Data *Accuracy* and *Reliability*
- **Availability**
  - Your data and resources are available when you need them



Importance of Cybersecurity in M&R

C
- Corporate Secrets
- Sensitive Equipment / SCADA

I
- Compliance / Auditing
- Maintenance Records

A
- Preventative Maintenance
- Resource Allocation

How Secures Is Your Data and Information...

Easy, right?

State Government

Government

OVERVIEW

A State-Level Government Agency responsible for onboarding technology solutions for various agencies throughout the state.

RISK

- Confidentiality of sensitive and confidential information
- Perception that utilizing SaaS solutions is more secure and doesn't need IT/Security review
- Compliance with NIST 800-53 Cybersecurity framework
- Shadow IT – network devices that utilize a non-approved or out of band communication method

SOLUTION

- All data, at rest and in transit, must be encrypted with modern and supported protocols
- Implementation of a Governance, Risk, and Compliance (GRC) solution to manage risk and processes
- Standing mandate that all network devices must go through a review to be approved for use on the State network – alternative commutation methods (cellular, hotspots) are not allowed

NIST National Institute of Standards and Technology

"As the government becomes more cybersecurity aware, we are responsible for evaluating the security posture of our vendors with a repeatable and consistent process. When our state agencies work with us to evaluate partners and solutions, the outcome is more likely to be beneficial to everyone while ensuring the privacy and security of our data."

Healthcare

Healthcare

OVERVIEW

A medical research center with wolrd reknowned scientists & researchers dedicated to prevent, diagnose and treat cancer, HIV/AIDS and other diseases.

RISK

- Vendor selection for data collection
- Type of data source is a key factor of vendor selection approval
- IoT devices that utilize a non-approved or out of band communication method
- Cybersecurity used in context of CMMS and IoT devices

SOLUTION

- Prior working with the vendor, questionnaire is required to review IT requirements, supported protocols, and exceptions
- Compliance with HIPAA is mandatory
- VP approval for all IoT project and exceptions (Exceptions need to be reviewed every year)
- Outbound communication method preferred
- Cybersecurity for CMMS/IoT devices is not the only issue, bandwidth must be expanded to support needs

Manufacturing

Manufacturing

OVERVIEW

A Global IIoT products manufacturer and services provider.

RISK

- Securing Sensitive PLC / SCADA systems
- Availability of Information Systems
- Compliance with NIST 171 / DFARS and navigating changing requirements
- Patching Cadence – keeping secure while minimizing downtime

SOLUTION

- Data encryption and segregation of networks
- Partnering with solution providers that have strong Business Continuity and Disaster Recovery programs
- Dedicated compliance and security teams
- Scheduled downtime – Preventative Maintenance for your IT Security

> ”The most difficult aspect of maintaining cybersecurity in the manufacturing space is navigating the push and pull between implementing the necessary security controls and maintaining our production throughput. It is key that the business understands the importance of managing the risk inherent with digital transformation.”

IIoT & Cybersecurity Considerations

1. Equipment

Evaluate your existing assets; software, hardware, data collection, analytics tools, and processes.

- ❑ Do you have real-time visibility into current operations?
- ❑ Are you able to predict maintenance issues?
- ❑ Are all endpoints secured?
- ❑ What about your legacy equipment?
- ❑ How old are the devices and systems you're currently using?
- ❑ What will need to be replaced?
- ❑ Which assets can be adapted?
- ❑ You'll want to determine if you have the technical assets in place to capture and store this influx of data, and if not, what will you need to put in place to make it happen?

2. Communications & Protocols

After you've developed a sense of what devices are included in your system, you'll need to consider how to configure those devices and how they'll communicate with each other. Communication must be both consistent and secure.

- ❑ How will you communicate with the devices?
- ❑ How will devices communicate with each other?
- ❑ Where do you currently get your internet from?
- ❑ How much coverage will you need?
- ❑ What are your data rate requirements?
- ❑ Energy efficiency requirements?
- ❑ What are the protocol security requirements?

3. Environment

Next, you'll want to assess your environment. You'll need to consider everything from the location itself to any potential issues, equipment, and installation logistics.

- ❑ Where is the facility located?
- ❑ How much space will your system cover?
- ❑ Will it be contained in one building or distributed across several miles?
- ❑ Are there multiple sites to consider?
- ❑ If the equipment is in a remote location, can each device be monitored via cellular networks?
- ❑ What are the on-site conditions? Humid? Dusty? Temperature-controlled?
- ❑ Does the equipment vibrate quite a bit?
- ❑ Are there safety hazards such as potential gas leaks? Dangerous equipment?

4. Security

How will you protect sensitive data?

- ❑ What existing measures are in place for capturing, monitoring, and storing data?
- ❑ Is your industry subject to any data protection regulations?
- ❑ Do you have a process for maintaining device security?
- ❑ A strategy for securing your network and detecting threats?

Key Takeaways

- The right people and controls must be in place to protect the confidentiality, integrity, and availability of your data.
- Operations/Maintenance must understand the sensitivity of the data under their care.
- Operations/Maintenance and IT must work closely together.
- What compliance frameworks is your industry subject to (HIPAA, ISO, SOX, etc.)?
- IIoT & Cybersecurity Considerations customer checklist.
- The Human Element

POLL QUESTION No. 2

What cybersecurity or IT factor is most important to your business?

(Click only one answer)

- Keeping all data on premise (no cloud solutions)
- Availability of your data when and where needed
- Regulatory Compliance (HIPAA, NIST, ISO, SOX, etc)
- Assignment of a data owner or administrator to the solution

“IoT without Security = Internet of Threats.”

- Stéphane Nappo, CISO of OVHcloud

FLUKE®
Reliability

Questions

QUESTIONS?

Thank you!

Frederic Baudart & Matthew Hudon

frederic.baudart@fluke.com

matthew.Hudon@fluke.com

FLUKE Reliability

Next webinar June 16: How to cope with the skills shortage

Suzane Greeman

Future-proofing asset dependent firms against the tide of talent flight

BEST PRACTICE WEBINAR | Wednesday, June 16, 11 a.m. ET

Talent risks now represent a significant threat to asset dependent firms. In addition to the sheer unavailability of talent, there is the increasingly competitive environment to attract talent.

The stark reality is that even where the talent is available, significant onboarding is required to hone troubleshooting and other skills that these firms rely on daily.

In this webinar, veteran asset management advisor and instructor, Suzane Greeman will break down the complexities surrounding the competences and talent that industry needs. She will also outline some creative ways in which talent acquisition and retention practices need to change to manage these talent risks.

To learn more about Fluke Reliability and our Webinar Series

SURVEY

Please provide feedback on this webinar by responding to our survey. Do you want a Certificate of Attendance?

WEBINAR SERIES

Visit this page to learn more about our Webinar Series: https://www.accelix.com/community/best-practice-webinars/

DEMO

Visit Accelix.com for a free demo of our Connected Reliability Framework.

FLUKE Reliability

FLUKE®
Reliability

THANK YOU!