INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

How to Tell If You Are Experiencing a Cyber Incident

Joe Weiss, Managing Director of ISA99, told me in a recent email, "It is not possible to have an effective OT/ICS cyber security program if you can't identify control system incidents as being cyber-related. Yet, OT cyber security is under the purview of the CISOs whose focus is the malicious compromise of IP networks and whose staff are not trained to identify control system incidents as being cyber-related."

This is a huge potential problem. It is important for the IT cyber security team to be relentless in stopping the cyber events that IP networks are exposed to—phishing, man-in-the-middle, unauthorized access, and all the other malicious acts that can beset a corporate entity.

The problem is that most cyber security personnel are IT centric and IT security oriented and trained. Many of them wouldn't know an OT cyber event if it came up and bit them on the leg. Most C-Level corporate officers are much more concerned with email issues, phishing, blackmail, and large scale theft of either funds or intellectual property. They don't see that OT cyber events can be even more critical than a simple IT event.

Part of the problem is that companies are extremely reluctant to disclose that they have been attacked in a cyber event. The reaction is still safety by obscurity, even though that has been thoroughly discredited for over twenty years now. Cyber physical events are not only occurring, but they are also relatively common. Perhaps they are not as common as IT cyber security events, but the numbers keep increasing.

Even so-called OT Security companies basically stick to the IP network and only pay lip service to the control networks and control elements and sensors. The control networks and their appurtenances, the common wisdom runs, don't have any real value to cyber criminals other than stealing the proprietary information in the data historians, which are located on the IP side of the networks, anyway.

ISSN: 2334-0789

A 1990s vintage HART based control valve might have been "too dumb" to try to invade, but today's transmitters and control elements are much smarter, and in many cases, directly connected to the IP network of the plant.

This had some partial validity years ago, when sensors and transmitters and control elements like control valves, compressors, injectors, and other devices were dumb or barely intelligent. A 1990s vintage HART based control valve might have been "too dumb" to try to invade, but today's transmitters and control elements are much smarter, and in many cases, directly connected to the IP network of the plant. IoT and IIoT networks can be located outside the traditional boundaries of the plant yet connected to the control system within the plant. This is a huge opening in the security barriers for the plant, yet most cyber security companies do not spend much time on them.

Sensors, themselves, and control elements, rarely if ever have cyber security built in. For example, smart power supplies are rarely protected, yet it is possible to use them as an entry point into the system. Oil and Gas Pipelines are vulnerable, as are power substations and transmission lines. Even many SCADA systems are very poorly protected against cyber intrusion, and cyber physical attack.

To give you an idea of exactly how bad the situation is, there has been only one control system designed from the ground up to be cyber secure. It was called Bedrock Automation, and it went out of business last year, through no fault of the management. Their corporate ownership killed it.

ISA, which has taken the lead in cyber security standards-making and education since before cyber was cool, has just issued a position paper titled "Advancing Industrial Cybersecurity." This paper points out that while cyber intrusions and their impacts have been exhaustively studied in banking, government networks and a wide variety of business networks, the impact of cyber attacks, especially cyber physical attacks, such as Stuxnet, notPetya, and Trisis, among many others, has hardly been studied at all. The paper avers that the impact of such attacks has been dramatic and disastrous from destruction of dams and safety control systems in petrochemical refineries to attacks on water distribution systems and wastewater systems.

Once again, at the base of this is the fact that most cyber security personnel, whether employed by an IT department or as a cyber security consultant, do not have the requisite knowledge of how manufacturing and process plants function, what components are critical, and what the effects on both the process and the business systems can be of cyber and cyber physical attacks.

After twenty years of pounding various podiums, people who ARE aware of the potential for damage and the damage vectors in process and manufacturing plants have not gotten through to enough people at the upper management or governmental level to be able to get people educated on these risks. Or to get them to quit minimizing them, or to get them to actually do anything about them.

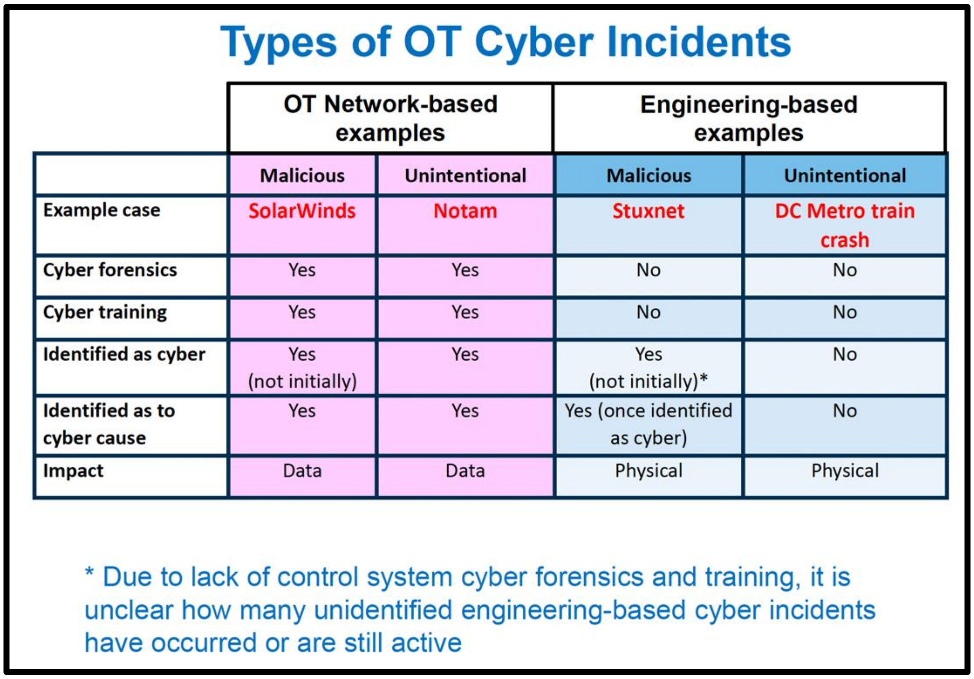
ISA continues to offer training on OT cyber security issues and generally approved good practice. Not enough people are taking them up on the training.

So, in addition to the position paper, ISA has approved the peer-reviewed Micro Learning Module (MLM) 38A – "Identifying Control System Cyber Incidents" - MLM-038-A-Identifying-Control-System-Cyber-Incidents-20230827.pdf , written primarily by Joe Weiss and his team at ISA.

This learning module essentially tells you how to know if you have been subjected to a cyber attack and what to do about it. And what to do to see to it that you don't get hit again. I've included a table from the learning module that shows several cyber physical incidents, including one which has never officially been labeled cyber (the DC Metro train crash). Note that while the network based incidents have cyber forensic trails, the engineering based incidents do not.

Even the most sophisticated sensors do not have cyber security built in. But here's the truth: it isn't too hard to do it. It can be done, and has been done, in the case of Bedrock Automation, and in the case of Adaptive Wireless Solutions, which I assisted in selling to Schneider Electric. AWS produced transmitters with 64 Gb of memory, complete cyber security protection, and the ability to record all instances of intrusion or tampering directly in the transmitter. If Schneider is doing anything with the company, I don't know about it. But they could produce an effective set of sensors and transmitters that were cyber secure if they wanted to. And if they can, other companies could, too. In both

Bedrock and AWS, costs were similar to those of any other sensor or control system manufacturer, so the issue isn’t that it is too expensive to adequately protect the field instrumentation like we protect the plant IP networks.



Types of OT Cyber Incidents

	OT Network-based examples		Engineering-based examples	
	Malicious	Unintentional	Malicious	Unintentional
Example case	SolarWinds	Notam	Stuxnet	DC Metro train crash
Cyber forensics	Yes	Yes	No	No
Cyber training	Yes	Yes	No	No
Identified as cyber	Yes (not initially)	Yes	Yes (not initially)*	No
Identified as to cyber cause	Yes	Yes	Yes (once identified as cyber)	No
Impact	Data	Data	Physical	Physical

* Due to lack of control system cyber forensics and training, it is unclear how many unidentified engineering-based cyber incidents have occurred or are still active

No, I believe that the real issue is that managements do not believe that OT cyber physical attacks can be so devastating that the global economy could be wrecked.

We KNOW that the global economy is fragile. Now that the effects of the global pandemic are coming to an end, we see just how fragile the supply chains of manufacturing and process plants around the world really are.

Maybe it won’t take a huge cyber-initiated disaster to get managements and governments doing the right things. Maybe.

Joe Weiss and the INSIDER Interview for October

The INSIDER Interview for October was a little longer than usual, but that was because the subject, cyber security, was important and the interviewee, Joe Weiss Managing Partner at Applied Control Solutions LLC, was extremely knowledgeable. The interview was a far-ranging discussion of the differences between IT and OT networks and systems and how to deal with the differences.

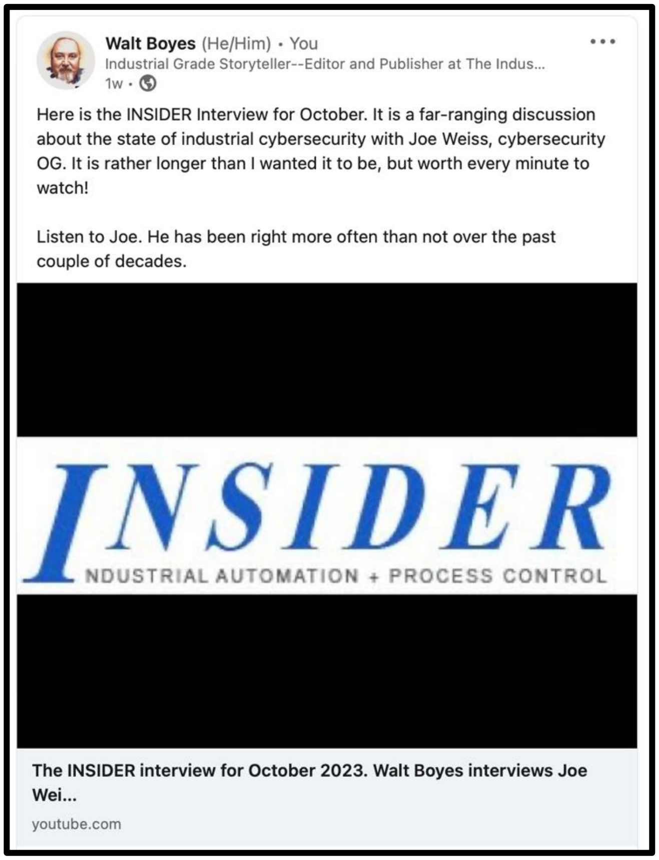
INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

Joe Weiss is a Cyber Security OG and was doing cyber security when there were maybe ten people with anywhere close to his expertise, even if you added me to the list.

Joe has been keeping a database of cyber incidents in manufacturing, utilities, power, and process control for nearly twenty years now.

Joe is Managing Director of ISA99, the cyber security standard committee. He is a PE, CISM, CRISC, and a Life Fellow of ISA. He is also a Senior Member of IEEE.

The interview can be found at https://www.youtube.com/watch?v=vwVwBqikmkM.



Walt Boyes (He/Him) • You
Industrial Grade Storyteller--Editor and Publisher at The Indus...
1w •

Here is the INSIDER Interview for October. It is a far-ranging discussion about the state of industrial cybersecurity with Joe Weiss, cybersecurity OG. It is rather longer than I wanted it to be, but worth every minute to watch!

Listen to Joe. He has been right more often than not over the past couple of decades.

The INSIDER interview for October 2023. Walt Boyes interviews Joe Wei...
youtube.com

AI and Sales and Marketing

With all the hooforaw and folderol about AI being a problem that might destroy humanity, I'd like to note that while there are things we CAN do, like training AIs to mimic human beings, there are things we SHOULD NOT do, like training AIs to mimic human beings. This is especially true in sales and marketing, where AI chatbots are already widely used and misused in customer service applications. It must not just be me, but it drives me crazy to have to argue with an AI to get to speak to a real human being who might be able to solve my problem instead of going through a rote decision tree in the hope that I might give up and go away, thus saving the company money on repairs and maintenance. You think?

Fact is, people are already getting fed up with chatbots even when they sound like they could beat the Turing Test with one braincell tied behind their backs. And there is even an early warning signal. Walmart and other large retailers are taking out the AI powered self-checkout stations that were introduced with enormous fanfare just a few years ago, because people are refusing to use them, and they have not been successful in

ISSN: 2334-0789

countering the increases in theft and other losses caused by mistakes in the self-checkers. I know that I am not alone in refusing to use the stupid things. This may be the canary in the coal mine about using AI chatbots and ChatGPT and its fellows to replace human expertise in customer and technical service and in copywriting and even in writing scientific papers.

The famous science fiction writer, Frank Herbert, in his monumental work, *Dune* sort of tossed off that centuries before, there had been something called the "Butlerian Jihad." This "holy war" was against "machines that think like a man." As a futurist, I have to look at that as one possibility.

WALT BOYES is a principal with Spitzer and Boyes LLC. He is a Life Fellow of the International Society of Automation, a Fellow of the Institute of Measurement and Control, a Chartered Measurement and Control Technologist, and a member of the Association of Professional Futurists. From 2003 to 2013 Walt was Editor in Chief of *Control* magazine, and from 2014 he has been Editor and Publisher of the INSIDER. From 2016 to 2022 he acted as Editor of the alternate history magazine, *The Grantville Gazette* and as Editor in Chief of *Eric Flint's Ring of Fire Press*. He recently joined Top of the World Publishing, along with Joy Ward, as SFF/AltHist Editors for their *Novus Mundi Publishing* imprint. Walt "pays it forward" as Vice-President of The Heinlein Society.
Walt is available for consulting and for speaking engagements both in person and online. Contact him at waltboyes@spitzerandboyes.com or waltboyes@gmail.com , or by phone at +1-630-639-7090.