

INSIDER

INDUSTRIAL AUTOMATION & PROCESS CONTROL

AN APOLOGY:

This issue of the INSIDER is horribly late. So late, in fact, that I've made it a double-issue (July/August). As you know I've been dealing with my wife, Joy Ward's illness, my own sudden trip to the ER and then for a week or so, with my Macbook Pro's illness.

My apologies to the readers of the INSIDER for this delay. I hope you will understand.

IN THIS ISSUE:

- **An Apology**
- **The Ineffable Fragility of Complex Systems**
- **The 21st Century Marketing Blues, Part SIX**
- **A Modest Proposal on OT Cyber Security**

THE INEFFABLE FRAGILITY OF COMPLEX SYSTEMS

Anybody who has tried to do something as simple as transfer money from one account to another, or buy an airplane ticket, or do any other other financial transaction in the last month has found out a great lesson thanks to two global outages of Microsoft systems and the apparent failure of CrowdStrike to adequately test their software updates. The lesson is that the banking system is very fragile.

For the Seattle Public Library most of the summer has been consumed by restoring computer systems after a successful ransomware attack, once again showing the fragility of the global library interconnected systems.

There are many more examples, and we can all think of them. They are all intimately caused by or connected to complex systems and their failure.

According to Wikipedia, "a complex system is a system composed of many components which may interact with each other. Examples of complex systems are Earth's global climate, the human brain, infrastructure such as power grid, transportation or communication systems, complex software and electronic systems, social and economic organizations (like cities), an ecosystem, a living cell, and, ultimately, for some authors, the entire universe."

Basically, a complex system is one whose behavior is greater than the sum of the behaviors of its components. Complex systems can be made up of other complex systems, each of which can have nested within it more complex systems.

INSIDER

INDUSTRIAL AUTOMATION & PROCESS CONTROL

Great. Now what does that have to do with Operations Technology? We may not think of the physical, electrical, electronic, and software components of an oil refinery to be a complex system, but in fact, a refinery is made up of numerous complex systems that interact with each other. As they interact they create issues that are not possible to correct within a single system.

This may, in fact, be one of the principal reasons why OT Security is simply not working. More on this later in this issue.

We need to look at complex systems *as* systems. We can't just look at them as a bundle of components: a pump, a valve, a set of sensors. While we need to treat these as individual components when we repair or do predictive maintenance on them, we need to see them as part of a system. A control loop is not by itself, either. It, too, is part of a greater complex system, which is probably part of an even greater and more complex system. So, if you turn off a valve in one place and an entire production unit goes down, this is an example of failure

caused by the interrelatedness of complex systems.

We have created this problem of interlocking complex systems by looking at systems and saying, "Look, we can combine them and they will work better and we won't have to work so hard." Bad idea!

The more complex the system is, the harder it is to control and maintain. Even though the analogy is not entirely correct you can think of a complex system as a finely tuned mechanical watch. It only needs a speck of dirt to become unstable and eventually fail.

Failure in a single system can concatenate and cause progressive failures of many interconnected systems.

In other words, complex systems are inherently unstable. Since we have a world that is full of interrelated complex systems, and which "*grew like Topsy*" instead of being planned for and designed, we have a world that is very much like a game of Jenga. You can pull out sticks until one too many comes out and then the entire edifice comes down.

We are very close to that level of instability on a global scale. What we need to do is to start thinking about how to lessen the complexity of global systems, and "harden them" so they can survive anything that comes at them. The classic example of doing this is the Internet itself.

INSIDER

INDUSTRIAL AUTOMATION & PROCESS CONTROL

Designed by DARPA to decentralize communications in the event of a nuclear war, the Internet found itself widely useful and widely used because of its design.

We have created this problem of interlocking complex systems by looking at systems and saying, “Look, we can combine them and they will work better and we won’t have to work so hard.” Bad idea!

If we want our interlocked global economy to last, and survive political and social threats, we are going to have to deconstruct the complex systems we have created. That will be hard but it is something we must do.

I don’t know about you, but I think that playing Jenga with our economy and our very lives is silly and stupid. We need to get a handle on this before it gets a handle on us.

THE 21ST CENTURY MARKETING BLUES, Part Five: Proactive Reputation Management

We have talked about defensive reputation management before, in the case of Boeing, and British Petroleum (now BP).

We can add to the cautionary tales the behavior of CrowdStrike after their software update basically killed the entire web, producing the single best advertisement for Apple Macintosh computers ever done.

At first, CrowdStrike was very unwilling to apologize, and offered some lame premiums for companies that had been seriously hurt. It was only after lawsuits were threatened and filed that CrowdStrike understood that they had produced a potentially company ending issue. Suddenly, the reputation management consultants were obviously consulted, and CrowdStrike’s responsiveness and attitude had a wrenching adjustment.

Proactive reputation management requires you to take a very honest look at your company and yourself and decide what you and your company stand for.

The jury is still out on CrowdStrike’s ability to survive this widespread catastrophe. We will see what happens in the next year or so.

INSIDER

INDUSTRIAL AUTOMATION & PROCESS CONTROL

But those examples are the negative aspect of reputation management. The question is, what do you do if you haven't made any noticeable mistakes, your reputation is good, and you want to make it better and continue to burnish it?

Now, this must be distinguished from mere marketing. Proactive reputation management requires you to do more than tout your products and services. Proactive reputation management requires you to take a very honest look at your company and yourself and decide what you and your company stand for. Unless you know the bedrock above which you stand, and on which your company is built, you cannot accurately describe who you are to anybody who wants to know. If you can't, in a crisis situation you will sound wishy-washy at best, and at worst, like you have secrets to hide.

Once you know who you are, you need to know what you stand for, and what your staff and customers think you stand for. If there is cognitive dissonance between what you think you stand for, and what your

people and customers think you stand for, you've got a real problem and you have to do something to fix it.

But once you know who you are, you can work on getting the world of customers, competitors, stakeholders and bystanders to know who you are.

Most articles about reputation management start when your company's been dropped in the dumper and describe ways to stay as clean as possible and get out of the dumper as fast as you can. This one is about what happens when you aren't in the dumper, and how to make sure you stay out of it.

Most articles about reputation management start when your company's been dropped in the dumper and describe ways to stay as clean as possible and get out of the dumper as fast as you can. This one is about what happens when you aren't in the dumper, and how to make sure you stay out of it.

You need to do a deep dive survey of your customers, competitors, and stakeholders. You cannot do this with a focus group. You cannot do this with an online survey. This is expensive but the dividends it pays are well worth it. You need to do a one-on-one, face-to-face interview with a statistically valid number of customers, competitors, and stakeholders. We call this "The Mind of the Customer®" and Joy Ward has been doing this kind of interviewing for more than twenty years. The results are flabbergasting. This will tell you what your core values really are, and what to do to maintain them or change them for something

INSIDER

INDUSTRIAL AUTOMATION & PROCESS CONTROL

better. This is qualitative research, and you can take the data from this research and do quantitative studies based on it.

What you will find is that the best way to keep your company's reputation out of the dumper is not to get in it in the first place.

If you are interested in learning more about qualitative research, let us know.

A MODEST PROPOSAL ON OT CYBER SECURITY

Okay, look. Neither IT cyber security nor OT cyber security actually works very well. How do we know this? Take a look at the number of successful exploits against IT: the billions of names, addresses, and other personal information that keep showing up for sale on the dark web. We can see that no matter how hard we work at getting people to do just the simplest things to keep their data safe somehow it is never enough.

The fundamental issue that underlies all of cybersecurity is that it is overhead. It is cost overhead, but more importantly it is overhead in the minds of the workers. The workers in your plant or office are tasked with doing a job, and with some few exceptions, that job isn't cybersecurity. The model for cybersecurity has been to add a few more daily tasks to the workers' overhead. Change your password regularly. Do not respond to phishing emails. Do not respond to hinky phone calls. Don't visit illicit websites on the company's computers. Every single one of these tasks adds non-productive overhead to the workers' workload. And then there is the overhead from IT cyber security folks who insist on imposing corporate IT security standards on plant level OT operators. Some of these standards, meant to

The model for cybersecurity has been to add a few more daily tasks to the workers' overhead. Change your password regularly. Do not respond to phishing emails. Do not respond to hinky phone calls. Don't visit illicit websites on the company's computers. Every single one of these tasks adds non-productive overhead to the workers' workload.

impose better security on the plant, actually can cause real operational catastrophies. For example, requiring password security to use an emergency shut off. Don't tell me this doesn't happen still, because I know better.

The Bad Guys® know this, and they know that at some point in every worker's day, they will be busy or distracted, or just plain pissed off at the security overhead (I've called it Security Kabuki in the past) that they just don't do it. They bypass

INSIDER

INDUSTRIAL AUTOMATION & PROCESS CONTROL

passwords or change the password on the computers to “password” or “12345,” or something else to get around the security overhead because they just can’t tolerate any more overhead and still get their work done. Then the Bad Guys® strike.

There is a limit to the amount of extra overhead that a worker can tolerate. The fact is that workers are not paid to do overhead tasks...that’s why they are called overhead. If you give workers too much overhead to deal with, they will either shirk the overhead tasks or they will be less productive, or both.

So, here’s my modest proposal: stop doing cyber security by making the workers carry the load. Figure out ways to make our systems and plants intrinsically secure instead of band aid patching them.

If you liked this issue of the INSIDER and want to contribute to the work we do, please...Buy Me a Coffee!

<https://buymeacoffee.com/waltboyes>



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 past 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 served Top of the World Publishing, along with Joy Ward, as SFF/Alternate History Editors for their *Novus Mundi Publishing* imprint until the imprint was sold. Walt is now a freelance editor. Walt “pays it forward” as Vice President and Director of The Heinlein Society.

Walt is available for editing, 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.