INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

This month, we have two articles for you. The first is another in the seemingly unending articles about cybersecurity and why our efforts are failing drastically. The second article is about the Great Quitting, and how servant-leadership may be our way to the future of work.

It's Time We Got Serious about Cybersecurity in the Industrial Environment

Yes, I know. I wrote about cybersecurity a couple of months ago. I've been writing about cybersecurity since before I was Editor in Chief of Control magazine and ControlGlobal.com. That was a long time ago, but things have not changed for the better.

Recently, I read somewhere that we should stop focusing on trying to stop cyber-attacks, and instead focus on how to recover from them. That is, we should concede the playing field, and just concentrate on patching up the wounded and carrying off the dead. If you believe this, I have only two words for you: ***What rot!***

It's a good thing the Biden Administration doesn't agree with this, either. In June, the Biden Administration's Department of Energy offered a *National Cyber-Informed Engineering Strategy* developed by the Office of Cybersecurity, Energy Security and Emergency Response. As the title of the essay indicates, the concept of Cyber-Informed Engineering is the underpinning of the proposed US response to the probability of cyber-attacks in energy, manufacturing and other industrial verticals.

Many years ago, I attended a meeting called by Johann Nye, then of ExxonMobil, along with other ISA99 committee members. Shortly before the meeting ended, I volunteered to contact the then-Executive Director of ISA, the International Society of Automation, Pat Gouhin, to ask him if ISA would take leadership on standards and testing to give automation systems a stronger chance of being resistant to cyber-attacks. Pat agreed, and what we talked about eventually became ISASecure.

You see, the problem is that the large preponderance of control systems are not designed to be secure. They are designed to be open, easy to use, so that operators can use the controls without having to pass through a whole set of identity checks, especially in an emergency.

ISSN: 2334-0789

Controllers, PLCs, and other devices cannot have passwords because in an emergency in a plant, milliseconds count.

The vast majority of field instruments and final control elements still operate in an analog world, using 4-20 mADC signals, or even pneumatic ones. They didn't have to be designed to be cyber-secure. But now, digital fieldbus systems including WirelessHART can even be retrofitted to flowmeters, pressure transmitters, and actuators and other final control elements. PLCs and DCS controllers are potentially vectors for cyber infiltration. And as Joe Weiss and I have been saying for more than a dozen years, field instrumentation is rarely protected.

So, what is there to do?

The *National Cyber-Informed Engineering Strategy* gives a clue. This strategy has been developed by the Department of Energy for power generation control systems, but is instantly applicable to all control systems regardless of type. Here are the operational principles they came up with.

National Cyber-Informed Engineering Strategy's Organizational Principles:

- **Interdependency evaluation**
- **Digital asset awareness**
- **Cyber-secure supply chains**
- **Planned resilience with no assumed security**
- **Engineering Information Control**
- **Cybersecurity culture**

Organizational Principles

- *Interdependency evaluation*—Integrate input from multiple disciplines and operational departments (e.g., safety, quality, maintenance, chemical) to understand how digital misuse could affect their area of operations. This ensures engineers can adequately plan for risks introduced by system interdependencies that may be outside of the engineer's traditional purview.
- *Digital asset awareness*—Maintain a complete and accurate digital asset inventory, enabling engineers to track hardware, firmware, and software over time, and actively analyze the vulnerabilities that may reside within them.
- *Cyber-secure supply chain controls*—Use procurement language and contract requirements to ensure that vendors, integrators, and third-party contractors deliver products that meet design specifications and adhere to organizational processes and controls that support cybersecurity.
- *Planned resilience with no assumed security*—Expect that any digital component or system may be compromised at some point during its lifecycle, and plan for continued operation during and

ISSN: 2334-0789

after a cyber attack that degrades digital controls. Implement a zero-trust architecture to the greatest degree possible.

- *Engineering information control*—Protect sensitive engineering records—including requirements, specifications, designs, configurations, testing, etc.—that if released may provide attackers critical information that places those systems at greater risk.
- *Cybersecurity culture*—Build cybersecurity into the organizational culture by leveraging a cross-functional and cross-disciplinary team to consider cyber-related concerns in the system design and implementation. Adopt continuous cybersecurity training across the organization to collectively empower all staff to participate in cybersecurity.

These are pretty much what most cyber-aware OT analysts like me have been arguing for, and it is great to see the Administration putting its money where its mouth is. All new plants should be designed using these principles.

We should replace every control system in every plant this is not designed to meet these principles.

We should replace every control system in every plant that is not designed to meet these principles.

But what about the brownfield plants? Honeywell and Yokogawa started putting in DCS control systems in the middle of the 1970s. Some of these plants are still using them or significant parts of them. Azbil, formerly Yamatake, has been building replacement parts for Honeywell TDC systems for all this time.

Yes, we should replace them all. There are control systems on the market that are secure-by-design, and there are trainers to train a cybersecurity culture into your plants. But wait! You say. We can't afford to rip and replace thousands of control systems and hundreds of thousands of field devices!

I say you can, and you have to. Do the math. Let's say your control system is in a refinery. Let's say it would cost $10 million to replace the system. How much would it cost to repair the system after a cyber-attack and how much would it cost in terms of lost productivity for months while the plant is put back together?

This is the cost of cyber security. We can either do it now, or we can let the bad actors make us do it after the attacks.

ISSN: 2334-0789

INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

Have you considered the concept of servant leadership?

The funeral of Queen Elizabeth II this week brought up a lot of thoughts about leadership. During her 70-year reign, she carefully guided the monarchy and the Commonwealth from a fractured Empire that was breathing its last to the modern Commonwealth as a free association of equals. In fact, in his homily at the funeral, the Archbishop of Canterbury made a point of calling out Elizabeth for *servant-leadership*.

Servant-leadership has been around for a long time. There is a story in the New Testament in which Jesus washes the feet of his disciples. That is an example of servant-leadership.

Robert Greenleaf said, in his 1970 essay, "The Servant as Leader": *A servant-leader focuses primarily on the growth and well-being of people and the communities to which they belong. While traditional leadership generally involves the accumulation and exercise of power by one at the "top of the pyramid," servant leadership is different. The servant-leader shares power, puts the needs of others first and helps people develop and perform as highly as possible.*

This is highly opposed to traditional top-down leadership in which income, benefits, and training trickle down to the lower echelons of the organization.

During the pandemic we were treated to many examples of servant-leadership as leaders found it necessary to encourage, coach, remind, cajole their remote employees (some working remotely for the first time) that doing the business of their enterprise was important, even when the diapers need changing. Servant-leadership leads inevitably to concentration on work-life balance issues.

This made typical corporate leaders cringe and as soon as they could assert their top-down power, they started making people come back to work in the offices. Suddenly, they found themselves with very short staffs. People who have experienced remote, non-punch-clock-based work didn't want to go back to showing up just so the boss could make sure they were working. So, the Great Quitting began, and hasn't stopped yet.

ISSN: 2334-0789

Servant-leadership suggests that everyone in an organization is important, from the line worker to the janitor to the C-suite. It also suggests that no one in an organization is that much more important than the "least" member.

This immediately leads us to consider the role of compensation. A servant-leader as CEO would not be comfortable making 200 times more than the janitor. At this point, we need to decide how to deal with this—because the Great Quitting is still ongoing.

One way is to cut the CEO's salary drastically but continue to pay the lowest ranked workers the lowest wages. Unfortunately, all that does is to spread the pain to the C-suite. Now, everybody is underpaid.

A servant-leader as CEO would not be comfortable making 200 times more than the janitor.

A servant-leader would ask why we don't put all the remuneration money into a big pool, and pay everybody a living wage, including the CEO. Perhaps there would be reasons why a janitor should not make as much as a CEO. But 200 times more?

Look at your organization. If you are continually having turnover in employees, and you can't hire fast enough to replace them, it isn't the potential employees' fault, is it? Of course not. It is management's fault, and if you are management, it is YOUR fault.

The huge growth in unionizing businesses that have never been union shops before should tell us all something about the current leadership of many companies. A top-down leader would solve this by paying better with better benefits than the union contract. A servant-leader would work with the unions to really improve pay and working conditions. Maybe even put union members on governing boards. The comment is always that the CEO and the board are risking their capital and that of the shareholders. But rarely is it asked what the workers are risking at the same time. It may not be large amounts of money, but it is their health, their career, and their priceless time.

But rarely is it asked what the workers are risking at the same time. It may not be large amounts of money, but it is their health, their career, and their priceless time.

ISSN: 2334-0789

INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

Nowhere is it written that a capitalist enterprise must be organized for only the benefit of the leaders and shareholders. A capitalist enterprise can, and perhaps should, be organized for the benefit of all its members, no matter how exalted or lowly.

The faster we can transition to servant-leadership, the faster the Great Quitting will stop, and people will come to love their jobs like we always believed they did.

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*. 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.

ISSN: 2334-0789