INSIDER
INDUSTRIAL AUTOMATION & PROCESS CONTROL

Cybersecurity Isn't a Product or a Process—It's War!

It's time to admit to ourselves that mostly we're doing cybersecurity wrong. This isn't to say that the knowledge isn't there, or that the concepts aren't there, or that there aren't several hundred highly capable practitioners out there who know what they're doing to the extent that they are allowed.

But think. Ransomware proliferates, even in the manufacturing and process industries. The vectors are many, including insider activity, phishing, and other types of attacks. Most of the victims of ransomware pay up, which bankrolls the hackers to try again with another victim. Copyright protection of intellectual property is a joke. Performers must go on the road all year because their recorded IP is stolen as fast as they can post it. My own works, *The Instrumentation Reference Book*, and others, have been pirated so often my publisher doesn't want to reprint it.

We have lost the war against fraudulent emails and texts. The hackers sit where they cannot be got at, and they spam and spam and phish and phish, and they get into places where they ought not to be. The statistics indicate that it is getting worse, not better. People are now blocking whole sets of domains to keep from getting spammed, and if you are expecting any business or personal email or texts from those domains, lots of luck.

We are fighting the hackers to a draw—sometimes.

Power utilities, water and wastewater utilities, manufacturing plants, oil refineries, and chemical plants are literally bombs ready to be set off by cyber-warriors or cyber-thieves, or both.

And that's the problem. After two decades of fighting, commercial, industrial, manufacturing, process industries, and utilities both power and water/wastewater are still plagued by intrusion, banks and other financial institutions are regularly robbed, and the average citizen's private information is so commonly sold on the "dark web" that there are television commercials about it.

ISSN: 2334-0789

And we know that the infrastructure of the entire world is vulnerable to intrusion, damage, and destruction. Power utilities, water and wastewater utilities, manufacturing plants, oil refineries, and chemical plants are literally bombs ready to be set off by cyber-warriors or cyber-thieves, or both.

We have known this for over a decade. We know that we can affect physical equipment through cyber means. Aurora and Stuxnet taught us that. We know that we can commit acts of terrorism remotely. We know that it is not terribly hard to interfere with the operation of a refinery or chemical plant in such a way as to cause serious damage and explosions and fires.

…88% of corporate boards regard cybersecurity as a business risk, rather than an IT or OT problem. So, what do companies do to manage risk?

Recently, Gartner announced that 88% of corporate boards regard cybersecurity as a business risk, rather than an IT or OT problem. So, what do companies do to manage risk? They buy insurance, and they do what the insurance people tell them to do to mitigate that risk. In the case of cybersecurity, the mitigation strategies haven't worked all that well. Attacks have gone up in double-digits. ICS-specific vulnerabilities have increased by a whopping 74%.

At the same time, COVID-19 and remote working have accelerated the move to Industry 4.0 by years.

The problem with this is that remote working is inherently insecure—far more insecure than working behind a hard-core shield on a completely defended network inside the plant. But so is working in a brownfield plant that is decades old.

Many varied layers of electric, electronic and automatic controls were layered over the original operations of plants rather than entirely replacing those systems.

Most implementations of Industry 4.0 are based on existing implementations of industrial control systems that are deliberately and intentionally insecure. When these plants were built, some as long ago as 100 years, there was no need for cybersecurity. When they were built, there was no networking, and most of the instrumentation and controls were pneumatic in nature. Many varied layers of electric, electronic, and automatic controls were layered over the original operations of plants rather than entirely replacing those systems.

ISSN: 2334-0789

Now, the corporate boards, having declared cybersecurity a risk, are demanding that the IT and OT managers figure out how to defend their enterprises from external attack. Now that this has been going on for a while, there are corporations whose mission is to help defend enterprises from external attack. This is a very good thing. It is a far better situation than it was fifteen years ago, when Joe Weiss and I sat down to try to figure out how many qualified ICS security researchers and engineers there were.

The problem with this is that everything that is being done is basically defensive.

We defend against spoofed emails, against phishing attacks, against man-in-the-middle attacks on remote access for control systems, and we defend against network intrusion inside and outside the plant. We research vulnerabilities, and we continue to permit software companies to write software with massive vulnerabilities in them. We are getting fairly good at being on the defensive, but you can't win on the defensive.

Several control systems manufacturers have begun producing inherently safe and secure products, but those companies are small, and their market share is not large. But unless you have the ability and the wherewithal to rip out your existing control systems and install these new inherently safe and secure systems, this doesn't help you one bit. Nor does it reduce the actual or perceived risk to your plants and controls. The barbarians continue to be at the gates, and all we can do is to make the walls higher, thicker, and the gates stouter.

The barbarians continue to be at the gates, and all we can do is to make the walls higher, thicker, and the gates stouter.

Now the fact is, cybersecurity has improved dramatically in the past decade. The vaunted Russian hackers, who famously stole an election in the United States in 2015, have been fought to a draw by the Ukrainian security researchers. But cybertheft is still a huge issue. The Ukrainians continue to fight off attacks on water and power utilities by Russian hackers. The Ukrainians are, like the rest of us, on the defensive.

What this means is that the entire methodology of cybersecurity is wrong. We are always on the defense, and this should not be. We should be attacking, not just defending.

ISSN: 2334-0789

One of the problems we've had in cybersecurity is that many of the attackers are ensconced in countries where they are at least ignored, and mostly protected. Russia, China, North Korea, Pakistan, Afghanistan, all have extant hacking groups whose clear intent is doing harm to enterprises in other countries like the United States, the UK, the EU, and other countries around the globe. Because hacking is not considered an act of war, these groups are protected from most realistic responses. Where we could simply put a cruise missile through a dictator's window, we can't do that to these hacker groups.

Or can we?

We need an international agreement on cybersecurity that declares attack hacking to be an act of war, not just a crime, or a tort. We need to stop this plague of barbarians now and entirely. Forever.

If we don't, we can expect that more countries will give protection to hackers. More countries will use this absolutely asymmetrical form of warfare. More countries will see this as a way to create revenue, lots of revenue.

Let's call it what it is—cyberwar.

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. He also acts as Editor of the alternate history magazine, *The Grantville Gazette* and is 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 .

ISSN: 2334-0789