An Executive Guide to Cyber Security for Operational Technology

Securing critical assets in a digitally connected world

wurldtech
A GE Company

THIS PAPER IS FOR INFORMATIONAL PURPOSES ONLY AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2016 Wurldtech Security Technologies Inc. All rights reserved.

Reproduction of this material in any manner whatsoever without the express written permission of Wurldtech Security Technologies Inc. is strictly forbidden. For more information, contact Wurldtech.

Wurldtech, Achilles and OpShield are registered trademarks of Wurldtech Security Technologies Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products.

Wurldtech disclaims any proprietary interest in the marks and names of others.

Table of Contents

Unleashing the Opportunity of the Industrial Internet

In 2000, analyst firm Frost & Sullivan coined a term to describe the growth of integrating machines used in industrial settings with Internet-connected sensors and software that collect data from machines, examine the data and then apply it to operations to improve efficiencies.

They called it the Industrial Internet.

Consider it the Industrial Age meets the Information Age, where physical and cyber collide; where the Internet intersects with our basic human needs—like water, transportation, healthcare, energy. It's where industrial enterprises are seeing the potential life-changing benefits that enhanced intelligence and connectivity can bring to critical control systems.

The Industrial Internet is already transforming global industry and infrastructure—with the driving force behind this inevitable evolution being the promise of efficiency, data management, productivity, and superior safety. By 2020, an estimated 50 billion machines will be connected to the Internet. Through accelerated productivity growth, this digital migration could boost global gross domestic product (GDP) by as much as $15 trillion by 2030.[1]

That's why, in the context of the Internet of Things (IoT), we call this the Internet of really important things.

Connecting to the Internet is an unavoidable reality of business, and only those who adapt and evolve will be able to advance and continue to compete in the modern world. That means optimizing for the digital age and moving process equipment online. While it can feel risky, and change can be tough, great value (e.g., increased revenues, lowered costs, enhanced automation) can come from embracing the evolution, thoughtfully and securely.

Despite the fact the Industrial Internet is here to stay, it is, most importantly, where companies will find the best opportunity for growth today—and maybe the only opportunity. Already, the Industrial Internet is saving billions of dollars each year across the industrial world through efficiencies created by Internet connectivity, insight, and innovation.

Data by GE shows that by bringing together digital technology with its domain expertise across industries such as aviation, energy, healthcare and transportation, customers can achieve a potential 20 percent increase in performance.[2]

Think about it: A more digital oil field means better asset management and more productivity at every well. A more digital hospital means better, faster, more efficient healthcare. A more digital rail system means freight is delivered faster and at lower cost.

Believe it or not, you're already online

The Industrial Internet opportunity is staggering, and many leading industrial firms are investing to capitalize on its benefits. Gartner estimated in late 2014 that manufacturing, utilities, and transportation would be the top three verticals using IoT in 2015. Together, they would represent 736 million connected things in use. By 2020, utilities will move into the top position, followed by manufacturing and government, with a total of 1.7 billion IoT units installed.[3]

Digital technology combined with industrial expertise could achieve a 20% performance increase.

With an increasing number of interconnected devices helping to automate and manage operations comes greater security needs. Cyber security is in the news on a daily basis. It's top of mind. People want to know: Is their medical data private? Is their bank information safe? Is their credit card secure?

But when it comes to the industrial sector, why are so few asking about industrial cyber security? Could it be that they don't know what to ask?

In the industrial sector, there are two camps when it comes to online connectivity. The first camp is connected to the Internet, knowingly, purposefully, and with the ability to reap the manifold benefits of that reality. The second is also connected to the Internet, but unknowingly and to the possible detriment to business and safety. Both need protection.

There was a time when connectivity outside an immediate plant or factory network wasn't possible and control engineers addressed security issues with air gapping—a strategy to physically isolate a secure network from unsecured networks. By definition, an air gapped system is neither connected to the Internet nor any other system. Air gapping as a strategy, however, now seems questionable.

There was a time, too, in the 1930s, when France constructed the Maginot Line—a line of fortification stretching from Switzerland to Luxembourg. The French heavily fortified the line on the German border. Unfortunately, they left the Belgian border weakly fortified, leaving a back door for Hitler to exploit. France fell in less than six weeks.

Somewhat analogous to air gaps, the line was impressive and may have seemed impenetrable, but, in the end, was ineffectual against new warfare tactics and technology. Similarly, an air gap strategy presents an inherent risk. Not only are those that use one left unprotected from nefarious outsiders, but they're also defenseless against deliberate or unintentional insider mishaps.

The Maginot Line illustration also reinforces another critical point: much like the Belgian back door to France, back door vulnerabilities exist in operational technology, too. It's critical to be aware of the various access points to operational technology and the lack of fortification often found at these access points.

Companies must realize the value—from business, maintenance, and equipment vendor perspectives—of connecting systems and having routable access between enterprise and the control systems. They must also accept that malware has been developed—think Flame, Stuxnet, and BlackEnergy—to circumvent air gaps.

With something as simple as a flash drive or Wi-Fi connection, a malicious or inexperienced insider could infiltrate and infect critical systems.

And finally, they need to fully understand what's happening in their networks in order to protect them.

Security waits for no one, so don't wait for security

It's time to fully realize the benefits of the Industrial Internet—securely. Engage early with industrial security specialists who can help identify security weaknesses, prioritize areas for improvement, mitigate immediate risks, and reduce the overall attack surface of your network. Select a firm that can provide guidance in implementing purpose-built solutions for industrial and process control environments that can scale to accommodate complex ICS and SCADA systems and provide full network visibility, control, and protection.

Designed for the operational technology sector, these solutions should be able to inspect and control traffic that runs across distributed controls systems (DCSs), programmable logic units (PLUs), and other industrial devices at the application command level, as well as detect and block unauthorized activity. They should also interoperate with traditional or next-generation firewalls to provide the right design for your IT–OT security transition zone and best protect your processes and control systems—all without the need for network re-engineering or downtime.

Key Insights

- The Industrial Internet creates tremendous opportunity for efficiency, productivity and safety
- You are already connected
- Air gapping no longer exists
- Steps should be taken to reduce overall attack surface of the OT network

Securing the Industrial Internet

While related and often used interchangeably, the Industrial Internet and the Internet of Things (IoT) are not one and the same. The former is more specific and a subset of the latter. While IoT connects “everything” (and most commonly refers to consumer devices like cell phones, fitness wearables, smart meters, etc.), the Industrial Internet represents the convergence of industrial machines, data, and the Internet.

It’s where the Internet intersects with our basic human needs, such as water, transportation, healthcare, and energy; and where industrial enterprises are seeing the potential life-changing benefits that enhanced intelligence and connectivity can bring to their critical industrial control systems (ICS), including supervisory control and data acquisition (SCADA) and distributed control systems (DCS).

Beyond IoT’s convenience, what’s driving the inevitable evolution toward the Industrial Internet is the promise of asset availability, efficiency, and safety. That and the fact that connecting to the Internet has become an unavoidable reality of business.

By converging global industrial systems with the power of advanced computing, analytics, automation, and connectivity, the Industrial Internet is allowing companies—in healthcare, transportation, and energy—to make significant operational improvements and to better compete in the modern world.

Don’t be too late

While time and money gains make for attractive incentives to join the connected world, it makes sense, too, that industrial companies may be reluctant to make changes that could impact the integrity and availability of critical assets and systems. Especially when this new world might feel a bit like Alice falling down the rabbit hole into Wonderland—what’s big is small and small is big and everything has been turned on its head.

But unlike the White Rabbit who fears he “shall be too late,” companies have an opportunity to be on time to securing their future. It comes down to making the necessary changes to accept the invitation and the need for change.

One major constraint to protecting industrial systems is a misunderstanding of the difference between IT (information technology) and OT (operational technology).

Thing is, industrial device lifecycles are measured in decades and, as a whole, lack today’s security requirements. Take, for example, nuclear weapons management. It’s based on 1960s technology and, while it works efficiently and has thankfully been very secure, the task of bringing it fully into the 21st century has been daunting and difficult. That goes for all sorts of other legacy and perhaps more mundane industrial sector systems and infrastructures.

For the first time, oil rigs and factories and refineries are sending mission-critical data beyond their physical perimeters, as well as inviting modern performance-enhancing solutions to advance their business. They’re making the cyber transition, but as they do, they cannot leave their systems vulnerable to theft and vandalism.

Industrial efficiency vs. industrial security

As physical and cyber befriend one another, so, too, must efficiency and security. The two need not be at odds and, in fact, companies should factor both into the production cost-benefit equation sooner rather than later. But before they can secure anything, they need to know what that “anything” is.

One major constraint to protecting industrial systems—even for industrial companies themselves—is a misunderstanding of the difference between IT (information technology) and OT (operational technology). It remains a hazy area in terms of if and how the two overlap, where they diverge, and who, with regard to internal security teams, is responsible for securing what.

Here’s an easy—if overly simplistic—way to think about it. IT stores, retrieves, transmits, and manipulates data. OT uses that data to monitor, control, and operate physical devices, processes, and events. In the past, OT systems were not connected to the Internet. Today, everything’s

In an OT environment, breaches can have disastrous consequences.

changing and, because of that, not only must new OT vulnerabilities be addressed, but companies must decide who's to address them and how.

Confidentiality vs. integrity breaches

The difference between a confidentiality and an integrity breach in the industrial space is significant. Compromises to IT systems can mean loss of data or damage to corporate brand, reputation, and profits. In an OT environment, by contrast, breaches can have disastrous consequences, with attacks resulting in the breakdown of nuclear systems, rail management systems, and other systems critical for smooth societal functioning.

Take, for example, an airplane. A confidentiality breach of its data system may result in a hacker getting his hands on a passenger manifest. During an integrity breach of a control system, however, a pilot's navigation panel could start to show that the plane is traveling higher than it actually is. While data theft is extremely serious, loss of altitude (and safety) or possibly life trumps all.

Safety must be job one

Today's industrial organizations take safety seriously and have reduced people risks. But as the world rapidly connects devices and machines, it's time to assess security weaknesses as the first step toward ensuring better protection of people, processes, technology, and intellectual property.

Critical Infrastructure: an Aptly-Named Segment

A quick review of history reveals many a rise and fall—and in the best cases, rise again—of industry-changing global brands. But in too many cases, changing industry dynamics have felled a large number of major corporations. A missed cue here, a misread trend there, or simply changing too slowly to correct course can have disastrous effects. In fact, Fortune magazine compared FORTUNE 500 firms listed in 1955 versus those listed in 2014. Nearly 90 percent of companies on the 1955 listing are now gone!

Companies must move and optimize for the times. Today, that means greater connectivity.

Companies must move and optimize for the times. And today, that means greater connectivity. While that can feel risky and change can be tough, great value (e.g., increased revenues, lowered costs) can come from embracing it, thoughtfully and securely, rather than resisting, avoiding, delaying, or ignoring it.

Executive tips for securing operational technology

In September 2015, the Department of Homeland Security (DoH) published a fact sheet: ICS Cybersecurity for the C-Level. It entreats C-level executives in the industrial sector to put cyber security at the forefront of their plans, while also offering up some basic practical advice.

It speaks of the growing rate and sophistication of malware attacks, citing Havex and BlackEnergy as examples. Havex, which operates as a Remote Access Trojan (RAT), can inject unauthorized control commands onto ICS/SCADA devices and cause denial of service in critical infrastructure (e.g., water, energy); BlackEnergy, another trojan-type bug, can compromise Human Machine Interface (HMI) software to gain access to control systems.

The DoH fact sheet lists six questions that every C-level executives should be asking about cyber security.

The 6 questions are:

- What assets are at risk?
- What are potential consequences of a compromise?
- Who's ultimately responsible for cyber security?
- Is your ICS environment protected from the Internet?
- Do you have remote access to your ICS environment? If so, how is that monitored and protected?
- Are you keeping current on recommended cyber security best practices?

It also provided corresponding risk management concepts or strategies, advising organizational leadership to:

- Identify critical assets and perform a cyber security risk assessment.
- Assign a cyber security expert to set policies and enforce monitoring.
- Protect your network by NOT connecting to the Internet.
- Secure remote access via multiple defense layers (e.g., two-factor authentication, VPNs).
- Join the ICS-Cert Portal for alerts and incident reporting.

How bad things can happen

Looking at the DoH risk-management concept list, one thing is not like the others—NOT being the operative word.

The use of all caps by the DoH must have been for emphasis. As if the author wanted to be certain there was no misunderstanding. While isolating an industrial system from the Internet may be a security technique, should it be considered best practices? In this case, the DoH guidance seems not only overly simplistic advice, but also naïve.

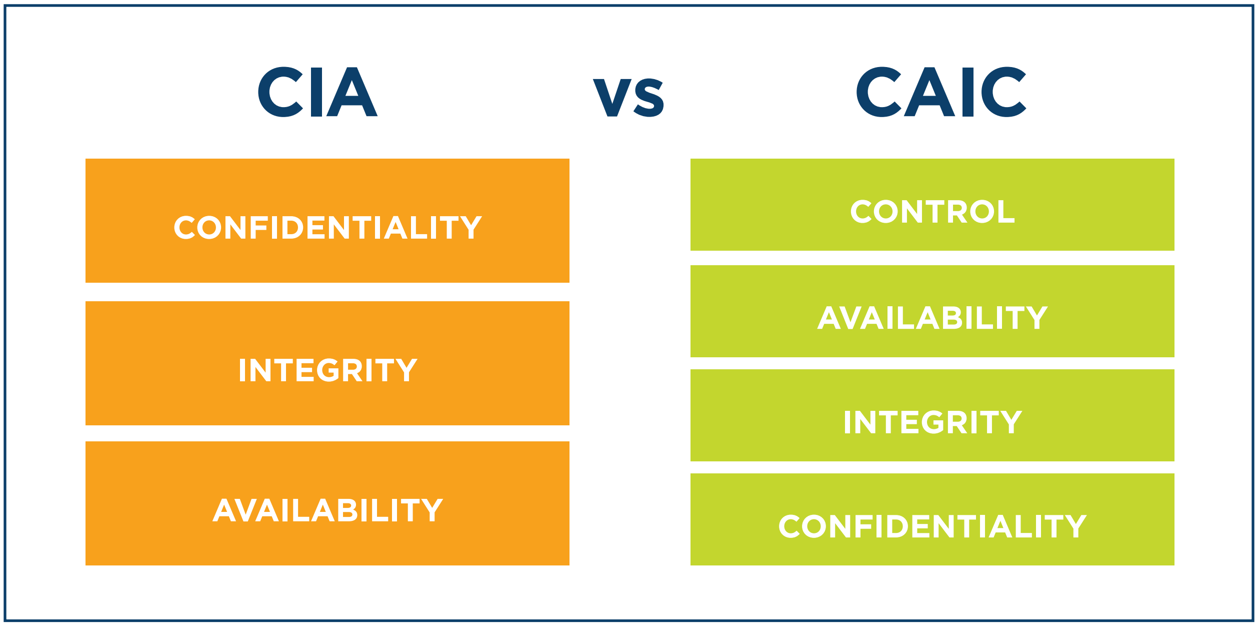
In this day and age, not connecting to the Internet is like telling someone the only way to avoid getting in a car accident is to not get in a car. Sure, that might work, but then where are you? Back in the 19th century? Forget all the advances the car industry has made in terms of safety. Heck, just don't ever drive or go for a ride again. Wouldn't it, as a best practice, be better to recommend use of seatbelts, going the speed limit, taking a driver's ed refresh, etc.?

Playing it safe is always a good plan, but living in a non-Internet-connected world is not. Even if organizations think they aren't connected to the Internet, they are. In some way. So more prudent advice would be to embrace and prepare for that truth (and its benefits) with the right people, the right tools, and the right training.

OT security and IT security: differences and opportunities

OT security and IT security are different, in several ways. But the most significant difference can be shown in terms of attack outcomes. An attack on IT could lead to data theft (ones and zeros); an attack on OT could affect the physical world (people, environment, assets). It's a serious distinction.

> In this day and age, not connecting to the Internet is like telling someone the only way to avoid getting in a car accident is to not get in a car.



CIA vs CAIC

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

CONTROL

AVAILABILITY

INTEGRITY

CONFIDENTIALITY

But while different, it is important to note that IT and OT security do overlap and converge. In fact, Gartner has an 80/20 rule-of-thumb[4] that says 80 percent of the security issues faced by OT are almost identical to IT (due to OT adopting IT technologies over time), while 20 percent are unique, not to be ignored, and critical (people, environment, assets).

Let’s break this down a bit and look at each according to: security and safety priorities, threat types, vulnerability lifecycles, air gapping and segmentation, available solutions, and staffing.

Security and safety priorities: CIA versus CAIC

In terms of security priorities, we can illustrate with CIA versus CAIC. Thanks to the likes of spy thrillers like James Bond and Jason Bourne, most folks see CIA and think Central Intelligence Agency. But in the IT world, CIA is the gold standard triad that drives security decisions and design policies. Ranked in order of priority, it stands for confidentiality, integrity, and availability.

By contrast, the OT benchmark is CAIC, standing for control, availability, integrity, and confidentiality. As is evident, OT cares about the same security properties, but ranks them differently and with safety forever being the top priority.

> When OT security fails, a digital attack can have physical repercussions.

Availability, for instance, becomes more important than confidentiality because of the nature of processes and the impact that shutting down and restarting systems can have on productivity. In some industries, shut down and restart procedures can take days.

Control, the added property, refers to the ability to control a process and change a state when needed and in a safe and secure manner. Because it can impact people, safety, and assets, it has to be the highest priority when considering the attack surface of any system.

Staffing skills for IT and OT

As with any emerging technology discipline, staffing can be a challenge. Most often, there is a clear demarcation between those who understand IT and those who understand control systems. The primary responsibility of IT is service delivery, often measured in service level agreements. The primary responsibility of OT is proper physical asset operations.

In the IT realm, there's generally more cyber security specialization. People have been specifically trained in application security or network security or encryption or any number of other important disciplines.

In OT, those tasked with security are usually operational technology people. As part of their day job, they have to deal with security, too. It's been an add-on, and not a specialization.

Vulnerabilities must be ranked differently and mitigations between discovery and patching must be more robust.

To achieve effective security, IT and OT can no longer be siloed functions; they must align. This makes collaboration and cross training essential. OT should have access to IT expertise, and IT must understand the needs of OT. If need be, they can start by focusing on baseline security such as identity and access control, asset management, and change management.

Threat types: data versus physical

If IT security fails, it has digital consequences (e.g., theft, vandalism, reputation damage, revenue loss). In OT, systems are not only used for information exchange and decision-making, but to change the state of a device or environment. That means, when OT security fails, a digital attack can have physical repercussions. Needless to say, the stakes are higher—people, environment, assets—when it comes to securing OT.

Because critical infrastructures are used by billions of people everyday, damage to them has the potential for economic, social, and political repercussions, including large financial losses or, even compromises to a country's sovereignty or defense. An attacker will claim to have compromised a substation or generation facility, threatening "lights out" if a ransom goes unpaid.

It's clear that the nature of attacks in IT versus OT is quite different in terms of priorities (think back to CIA versus CAIC). But, often times, the nuance isn't in the threat, but in the different approaches required to deal with threats when they are realized.

Vulnerability lifecycle: no "patch Tuesday" in OT

Because of the difference in threats and priorities, the vulnerability lifecycle in IT versus OT differs

significantly. In IT, the vulnerability lifecycle begins with the discovery of, well, a vulnerability—which often isn't until an exploit (e.g., malware in active attacks) reveals the software deficit. Once discovered, the immediate reaction is to give vendors an opportunity to create a patch. This fix process has become so commonplace that's it's almost a fact of life. Once the patch is installed, the issue is generally considered mitigated.

> Those who previously relied on air gapping to keep them safe are out of luck because air gapping no longer exists.

In the time gap between discovery, patch publication, and patch installation, technologies like IDS, antivirus, and IPS are used to mitigate the risk. And it's with that time gap where the major difference between IT and OT lies. In IT, the gap is relatively short—a matter of days, weeks, maybe months. In OT, because patch cycles tend to be much longer, the useful life of exploits can often extend to months and years.

This means vulnerabilities must be ranked differently and mitigations between discovery and patching must be more robust. For instance, a denial of service attack would likely be ranked a higher priority in OT than in IT. The same goes for a privilege escalation in a pre-authentication setting (common in OT control systems, but rare in IT); it would rank much higher for OT in terms of severity than it would in an enterprise software system.

The myth of air gapping

Prior to the Ethernet revolution of the 1980s, there was no connectivity possible outside an immediate plant or factory network. Systems were designed to be flat in nature. And the mindset of the control engineer was to respond to security issues with air gapping. By definition, an air-gapped system is neither connected to the Internet nor any other system.

Companies have since realized the value—from business, maintenance, and equipment vendor perspectives—of connecting systems and having routable access between enterprise and the control systems. And those who previously relied on air gapping to keep them safe are out of luck—basically because air gapping no longer exists. As seen with the latest malware, including Flame, Stuxnet, and BlackEnergy, modules have been developed to circumvent air gaps. With something as simple as a flash drive, a malicious or inexperienced insider could infiltrate and infect critical systems.

What's more, operators may not have policies for patching legacy OT systems that have been considered air gapped.

What to look for in solutions

In IT, information on threats and vulnerabilities is readily available. There is a rich marketplace of security vendors for firewalls, intrusion detection and prevention, application control, and many other areas.

OT security, on the other hand, is an emerging field. There is a smaller vendor set, as well as proprietary protocols. While off-the-shelf next-gen firewalls, for example, are valuable go-to solutions for IT, they won't work in OT. They're not designed for OT environments where the threats are different and repercussions of attacks more severe. New solutions are needed and they must be developed specifically for OT.

Moreover, there's not only a difference in solution availability, but there's a difference in creating a security solution that works in the mindset and culture of OT engineers who are used to highly intuitive, visual, drag-and-drop tools. Solutions must be purpose-built and optimized for them and if they aren't accessible and easy to use (UIs matter tremendously), no one will use them.

Vast Differences Between IT and OT Cyber Security

In the movie, *Wedding Crashers*, actors Owen Wilson and Vince Vaughn made crashing parties look easy, but the freeloading duo also weren't trying to crash Prince William and Kate's nuptials. Getting an invite to a celebrity wedding is much like getting on a whitelist. If you're on the list, you're golden—dance the night away. If you're not, you're out of luck and stuck reading about it in the gossip column or celebrity magazine on your next visit to the hair salon or grocery store.

Briefly put, whitelisting provides protection against malware (unwanted guests) by allowing only known good files (friends and family) to execute. Everything else is blocked. While not totally foolproof, it works well in environments where the stakes—people, environment, assets—are high.

On the flip side, there's blacklisting—what you'd find with traditional antivirus software. Blacklisting is a bit more reminiscent of the "Red Wedding" from *Game of Thrones*. To be sure, the Lannisters would never have made the guest list—and, in fact, would have been blacklisted from the affair. However, like morphing malware, they found a way in. And poor Robb Stark, who'd been lulled into a false sense of security, found out too late—when Roose Bolton plunged a dagger into his heart, saying, "The Lannisters send their regards."

There are all types of bad guys. Perhaps not all as despicably bold and evil as Roose Bolton and his not-so-merry band of assassins, but enough who have little concern for feelings or etiquette or humanity or anything other than their own prodigious plundering. Not to say blacklisting is without its merits (or that every wedding comes with the same life-and-death risks as those in Game of Thrones), only that it's not as fail-safe as whitelisting, especially in scenarios—transportation, nuclear reactors, power plants—where second chances aren't really an option.

Whitelisting vs. blacklisting

Whitelisting operates under the principle of deny by default, and this works well in more static OT settings where rule sets are shorter. If a software program doesn't have permission, it's not allowed to run. If something isn't exactly as expected, it's not allowed to run. Plain and simple: If it's this, allow it. If it's not this, do not allow it. The key is proper setup and maintenance to ensure there are no detrimental effects to not allowing.

When properly configured, whitelisting can be viewed as a more proactive approach that can stop most malware (including unknown malware) from being executed or even installed in the first place. That's not to say it's a set-and-forget, low-maintenance solution. It does require updating when software changes are made to a system and its primary challenge, again, is locking down systems as tight as possible for maximum security, but without blocking critical functionality.

When properly configured, whitelisting can be viewed as a more proactive approach that can stop most malware from being executed or even installed.

On the other hand, blacklisting only blocks known malware. Because of the iterative nature of malware attacks, this practice tends to become more reactive—again, chasing threats and responding to exploits versus patching vulnerabilities before an incident occurs. In IT, this can work because vendors are continually looking for and resolving vulnerabilities based on threats and exploits—which, generally speaking, aren't considered life threatening. For this reason alone, blacklisting isn't ideal for OT environments.

But wait. There's more.

Blacklisting also requires regular malware scans, which not only take up a large amount of processing power, but they take time. After control, availability is most critical. Systems can't be slowed down in order for a scan to run and they can't risk having antivirus software delete a file—that may contain malware—when, in fact, that file could be critical to a system running without disruption.

With a grain of salt, let's think back to the "Red Wedding." Roose Bolton and his crew were an iffy bunch—not necessarily a known good (whitelist) or a known bad (blacklist). But by choosing to accept them as not a known bad, Robb Stark let the enemies into the castle where they lied dormant until the signal to attack. Had Robb, instead, stuck to the safer, more traditional whitelist, it may have been a smaller party, but he and his family might have lived to see another day.

Different security for different environments

For critical infrastructure organizations, whitelisting is one of the top practices for protecting against harmful applications and mitigating targeted cyber intrusions. To better appreciate why, it's important to understand how both IT and OT environments work, and how they operate under different conditions.

IT vs OT

IT is dynamic

Comprised of fluid, intertwined technology stacks, IT has a lot of moving parts—which means it also has an incredible number of exploit variants. From network to compute to application to data and more, IT teams are responsible for safeguarding every layer in a stack with its own brand of add-on security (e.g., VPN, SEIM, NGFW, DLP).

On top of that, these security teams are caught up in a perpetual game of cat and mouse with attackers who always seem to have the advantage and be at least one step ahead. It's a never-ending cycle of identifying new viruses, updating malware signatures, closing security holes, etc.

OT is deterministic

OT systems are engineered for specific, measured, prescribed actions based on content, and not context. That's determinism. Things only happen one way—the way they were designed to act. If given a certain input, they will always produce a certain output, time and time again. It's an either/or. For example, you open a valve or you close a valve. There are no in-betweens.

No question, the OT threat landscape is scary, but because of its deterministic environment, the nature of attacks is not as dynamic as in the IT world—and the primary security focus becomes about ensuring control.

IT: Data is king

IT is about digital information storage, retrieval, transmission, and manipulation. Most businesses want to ensure smooth data flow. For example, Amazon wants to be sure identities are verified, that credit cards are working, and that searches and purchase histories can be used to offer up "you so need this, too" suggestions. None of these crosses over into the physical realm of process control and manual manipulation.

OT: Process is king

OT is all about process control, which is why it's not germane to think about things in the same way you would in the IT world, where defenses are layered (at times, seemingly ad infinitum) onto technology stacks. Industrial organizations typically run a small suite of control applications, and maybe a few more to help manage and maintain systems. For the most part, the environment remains relatively static.

IT: Gateways are everywhere

More gateways mean a larger attack surface. And considering that 60 percent of network traffic is bots, it's no wonder attackers only need to be right once—yet another reason IT guys are one step behind the bad guys. It's nearly impossible to keep up.

OT: Fewer gateways

Fewer gateways, fewer avenues for attackers to pursue. The key is reinforcing armaments at those known gates, moats, and tunnels from the start.

IT: Confidentiality is priority #1

In order of importance, priorities are: confidentiality, integrity and availability (the CIA triad). First and foremost, businesses and consumers expect financial, medical and personal data to remain private.

OT: Control is priority #1

In OT, an additional priority tops the list, while the rest are flip-flopped. The new order: control, availability, integrity, and confidentiality. Control equates to safety because, in this environment, loss of control could have dire consequences. Next is availability (e.g., we expect to have water at the flick of a faucet), then integrity (e.g., we expect that water to be clean and pure), and finally, confidentiality.

IT: Throughput matters

The amount of data that can be transferred at any given time is a big deal in the IT world, where connected constituents have gone all Oliver Twist, minus the "please, sir." That means both bandwidth (think of this as a multiple-lane highway) and throughput (the number of cars traveling on the highway at any given time) demands are ever growing.

OT: Throughput is secondary

The "information highway" infrastructure is less complicated and less congested in OT. If, say, a four-lane highway were built, it was done so because four lanes were more than adequate to handle the relatively fixed amount of anticipated traffic. Throughput requirements aren't changing as quickly or drastically as in the IT space.

IT: Patch Tuesdays

Security patching is so commonplace in IT that vendors have a regular weekly release day. Vulnerabilities are easy for attackers to find. They're also often only discovered as a result of an exploit. In fact, because of the dynamic nature of IT environments, it's becoming a rarity to find vulnerabilities pre-exploit.

The good news for IT is that, once found, vulnerabilities generally have effective patching available within days to mitigate damage.

OT: Patch...decade?

No matter what, security cannot make critical infrastructure less available or reliable. In fact, it cannot have any negative impact—no disruptions, no slow downs—to the real-time and deterministic operation of critical infrastructure.

So even if Patch Tuesdays did exist (which they don't), they wouldn't be a viable solution. It's just not feasible to drop security measures in and expect them to work as they might in IT.

When Facing Dangerous Enemies, Call the Professionals

From petty-crime hackers living in Mommy and Daddy’s basement to state-sponsored cyber sophisticates, there’s a wide range of marauders in cyberspace. Each with their own challenges; each with their own agendas and ideas of success; but all with a new and different target on the market. Today, the big prize, the pièce de résistance of cyber malfeasance is the industrial sector full of systems that were not designed with security in mind or at least not the type of security required to combat cyber crooks. It needs more than simple obstacles to channel the little guys in a different direction; it needs fully manned ramparts to deflect the more determined and well-funded foes.

Today, the big prize, the pièce de résistance of cyber malfeasance is the industrial sector.

In simpler terms: when it comes to OT security, call in the professionals. Because those bad guy adversaries are really smart.

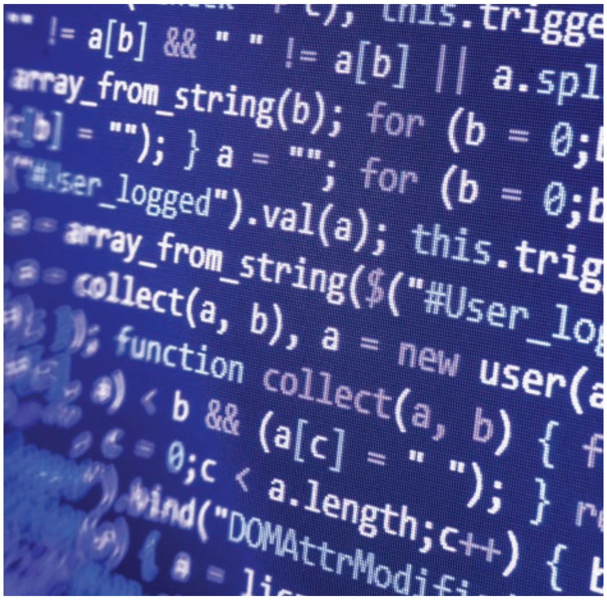
Who are the bad guys?

Attackers are a diverse bunch. They include, of course, nations states, but also other hackers, hacktivists, script kiddies, cyber terrorists, crime organizations, and insiders (malicious, exploited/tricked, and careless/accidental). Some are amateurs seeking a challenge or notoriety. Some are driven by political agendas or publicity. Some are highly organized, professional teams executing targeted and disruptive attacks with sophisticated tools for ransom, revenge, or worse. Many are well funded, especially when sponsored by nation states.

No doubt, motivations run the gamut. And no doubt, the industrial sector has become a new prime target.

- In summer 2015, it was revealed that China exploited the U.S. Office of Personnel Management, stealing the personal information of 22 million people. It's also believed that China stole the blueprints for the United States' F-35 stealth jump jet. While both were data breaches, the industrial sector should take serious note.
- In September 2015[5], U.S. National Intelligence Director James Clapper appeared before a U.S. House Committee on Intelligence hearing. SecurityWeek (and other news sources) reported Clapper's testimony in which he said unknown Russian hackers compromised product supply chains of several ICS vendors. According to reports, Clapper said customers of those vendors unknowingly downloaded malicious software with the intent by bad actors of exploiting facilities and operations.

Many hackers use pre-existing malware and adapt it to find and exploit network vulnerabilities.


), this.trigge
!= a[b] && " " != a[b] || a.spl
array_from_string(b); for (b = 0;
b] = ""); } a = ""; for (b = 0;b
#User_logged").val(a); this.trig
array_from_string($("#User_log
collect(a, b), a = new user(a
function collect(a, b) { f
< b && (a[c] = " "); } r
= 0;c < a.length;c++) { b
bind("DOMAttrModifi

A stark reality and scary proposition in today's world, where many attackers don't even have to develop their own tools. Instead, they can use pre-existing malware and adapt, for example, a popular hacker app like Metasploit, originally designed to automate penetration testing for cyber security professionals and ethical hackers, to find and exploit network vulnerabilities. It's a world, too, where attackers are targeting areas of weaker physical security such as radio links (Wi-Fi) by software-defined radio (SDR) hacks, fiber connections via fiber tapping, or systems with weak or non-existent passwords. It's a world in which "legitimate" companies, operating in unregulated grey markets, are in the business of selling zero-day vulnerabilities for SCADA systems.

If that's not chilling enough, consider the "destructive" attackers—those plotting to gain access of control of systems in order to inflict substantial physical damage. Destructive attackers who may be from any one of these outsider groups, or who could be lurking within the corridors and confines of your own organization.

The bad guys might be closer than you think.

Research shows that 85 percent of cyber attacks come from the outside[6]. However, it also indicates that malicious insider attacks, while more rare, are often more destructive.

In ARC's 2015 Industrial Cyber Security Global Market Research Study, participants ranked their primary concern as internal threats.

That's right. Bad guys aren't all faceless and nameless. The people who work for your organization are potential perpetrators. And this is perhaps why organizations are shifting their focus inside.

It's time to crack down on malicious—or just careless—insider threats.

In ARC's 2015 *Industrial Cyber Security Global Market Research Study*, participants ranked their primary concern as internal threats. Yes, that's above all variety of external threats—from cyber terrorists and criminals to unfriendly nation states and hacktivists. Perhaps counterintuitive, it was ARC's contention that while naivety regarding external threats is a possibility (especially when it comes to limited concern regarding wireless network and BYOD threats), it is more likely that organizations are more confident in their external perimeter defenses and are now looking to find better ways to "protect themselves from themselves." (And maybe also because many organizations' internal security measures are easier to bypass.)

But back to those insider threats. What constitutes a malicious insider?

As defined by Computer Emergency Response Team (CERT) at Carnegie-Mellon University, "A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."

Another study showed that employees make up 85 percent of internal threats.

Another study by the Software Engineering Institute of Carnegie Mellon showed that employees make up 85 percent of internal threats, while contractors, subcontractors, and business partners constitute the remaining 15 percent.[7] But to be clear, that doesn't necessarily mean that 85 percent of the damage derives from employees. Trusted contractors, too, can undermine an organization's security and destabilize core capabilities.

What's important is that practices, policies, and processes regarding cyber security be established, taught, and engrained in the psyche of not only full-time employees, but anyone who is granted (or may happen along) access to sensitive data and control systems. This includes vendors and sub-vendors who come and go all the time. They may arrive to manipulate, repair, or replace their own specialized equipment, but what else are they privy or given access to?

The incidents we know about

In June 2015, SANS Institute released its report, The State of Security in Control Systems Today. One third (34%) of respondents from around the globe said they believe their systems have been breached more than twice in the past 12 months.

Here are some of the most noteworthy attacks on critical industrial infrastructure.

Stuxnet

Discovered in 2010, Stuxnet targeted Iran's nuclear enrichment program. It infected 100,000 computers at 22 manufacturing sites and destroyed 1,000 centrifuges. Initially, it spread using infected removable devices. It exploited the controller architecture by hijacking a vendor's dynamic link library (DLL) driver.

Duqu and FLAME

Labeled the "sons of Stuxnet", Duqu and Flame happened, respectively, in 2011 and 2012. Duqu was Trojan horse malware that captured and exfiltrated data via a jpeg file. Flame was spyware discovered in Iran oil and nuclear installations. More complex than Stuxnet, it could record audio, screenshots, keyboard activity, and network traffic.

78 percent of security officials expect a successful attack on their ICS/SCADA systems within the next two years.

Shamoon

In 2012, Shamoon targeted Saudi Aramco, an oil and gas company, and was, to date, believed to be the most destructive business sector attack. It infected more than 75 percent of the oil and gas company's workstations, replaced crucial file systems with an image of a burning U.S. flag, and bungled messaging services for weeks.

Dragonfly

In 2013 and 2014, Dragonfly (a.k.a. Energetic Bear) targeted U.S., Canadian, and European defense and aviation companies. It used spam email campaigns and watering hole attacks to spy on, damage, and disrupt operations.

Other Significant Attacks

Though "unnamed," these incidents left indelible impressions.

In 2013, a malware-infected USB stick wreaked havoc on a U.S. power plant when it transferred a virus to 10 computers on a turbine control system network. Operations were impacted for nearly a month. The following year, a hacking group attacked a U.S. public utility's control system network through, it's believed, an Internet portal that gave employees access to the utility's control system. The hackers used brute force cracking to break the simple password mechanism. Also in 2014, another group used spear-phishing to infiltrate a German steel mill and prevent a blast furnace from shutting down. The fully digital attack resulted in massive physical damage.

Unfortunately, attacks of this nature are on the rise.

In fact, a 2014 Ponemon Institute study, *Critical Infrastructure: Security Preparedness and Maturity*, revealed that 67 percent of critical infrastructure companies suffered an attack—which led to loss of confidential information or disruption in operations—within the previous year. The paper also stated that 78 percent of security officials were expecting a successful attack on their ICS/SCADA systems within the next two years. What's more, according to Dell Security's 2015 Annual Threat Report, worldwide SCADA attacks increased from 91,676 incidents in January 2012 to 163,228 in January 2013 to 675,186 in January 2014.

These numbers are not looking very good.

Thanks to emerging companies who specialize in operational technology security industrials can better prepare for and defend against these types of attacks.

But what is looking good is the growing focus on the space and its differing security needs. Thanks to emerging companies who specialize in operational technology security, understand the threat landscape, and offer purpose-built solutions to address the complexities and potential vulnerabilities of greater connectivity, industrials can better prepare for and defend against these types of attacks and stand up to the new world of cyber criminals.

The threats you don't know about

It's incumbent upon any organization that is serious not only about its bottom line, but about safety and longevity, to engage the proper level of security expertise to protect core commodities and production processes. No longer will a last-minute frenzied call for emergency technical support suffice. The threats to critical infrastructure systems have advanced far beyond mischievous kids in their parents' basement. They require the skill and knowledge of industrial security specialists who can proactively man industry's bastions and continuously patrol its back alleys to ward off both outside and inside threats.

OT Security: Where to Start

Security requires taking a proactive stance to maintain health and prevent bad stuff from happening. In the industrial sector, a great place to start is with an overall site security assessment and health check that can uncover existing weaknesses, map out potential future risks, and recommend mitigation strategies.

In a 2014 ARC study, *The Future of Industrial Cyber Security*, it recommends organizations “focus on cures, not remedies.” (In this case, ARC seems to be saying a remedy treats a disease while a cure eradicates it.) As the study reveals, many existing control systems were developed prior to online security being as grave a concern as it is today. And while the need for compensatory controls and frequent patching (remedies) hasn’t gone by the wayside, ARC advises companies to invest more time and energy into developing new strategies that can cure (to the maximum extent possible) the underlying issues.

This is why security hygiene needs to be an organizational priority—and it requires the right game plan. First, emergencies need handling and weaknesses need uncovering. Next comes a treatment plan for any issues found and then it’s a matter of ongoing care and prevention.

> Security hygiene needs to be an organizational priority—and it requires the right game plan.

With a security assessment, companies can establish a baseline understanding of their existing security posture and begin to develop an effective long-term strategy for maintaining overall system health and hygiene.

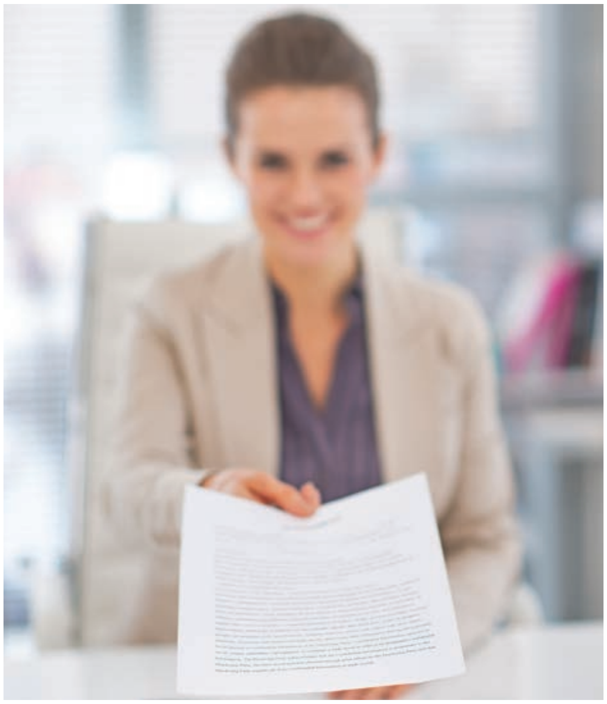
Keep it clean: industrial-strength security health

A typical assessment entails:

- Information gathering and documentation relating to an organization’s people, architecture, and technology
- Review and analysis of documents detailing network configuration, topology, policies, and other relevant aspects unique to an organization
- Onsite interviews and inspection with subject matter experts for additional technical and contextual understanding not apparent from documentation reviews alone
- Onsite technical testing to assess and evaluate the cyber security posture of assets
- Offline data analysis and application of best practices methodology to assess risks
- Risk assessment to identify sources of vulnerabilities, determine security posture, prioritize potential risks, and provide remediation roadmap
- Findings report to include recommended mitigations based on prioritized risks

Benefits of an assessment include:

- **In-depth visibility:** Discovery of current security posture via a comprehensive report and workbook that maps out the potential risks for each system analyzed
- **Actionable results:** Immediate security risk remediation as well as long-term financial planning and resource justification with analysis based on leading expertise in the operational technology security field



- **Enhanced security:** Best practices methodologies identify key risks and dictate necessary strategies for overall improved security posture

Next, install security solutions purpose-built for industrial and process control environments. Solutions should have a modular platform designed for scale to accommodate complex ICS and SCADA systems and provide full network visibility, control, and protection. And it should interoperate with traditional or next-gen firewalls to provide the right design for your IT–OT security transition zone to best protect your processes and control systems, all without the need for network re-engineering or downtime.

Finally, industrial customers should expect device manufacturers to certify that their products have passed stringent security assessment throughout the product development lifecycle.

Security first

Security cannot be an after thought. Once an assessment's been completed, with vulnerabilities found and patched, companies can also look to implement new rules and tactics and continue to build upon their game plans for keeping fit. These may include:

- Decreasing the use of commercial off-the-shelf systems that are easier to hack (the cost savings often aren't worth the risk)
- Forbidding use of personal devices in control rooms
- Requiring changes to default passwords on equipment
- Blocking off USB ports (Do you want a USB drive to be the downfall of your operation?)
- Enforcing rules where they already exist
- Implementing stricter pre-employment screening requirements
- Conducting property inventories and audits (on desktops, laptops, removable media, security tokens, access cards)
- Enhancing access controls for privileged users

Moreover, organizations should offer cyber security training programs that encourage dialogue—between engineers, contractors, everyone—to raise awareness of cyber security risks, including the dangers of setting up unauthorized Internet connections. Risk is everywhere, but can be reduced by enabling accountability, implementing least privilege access, and regulating sensitive control and data access.

Keeping up security hygiene isn't easy, but it's worth the time, effort, and justified expense to be safe.

Summary

The Industrial Internet promises great opportunity. A 20 percent[8] efficiency gain over 15 years could yield billions in savings annually across industries such as energy, transportation and healthcare.

But to fully realize its potential, the Industrial Internet must be secure. Strategies such as air gapping are ineffective at best, and can provide a false sense of security at worst.

The threats to industrial environments are real and growing, including small-time thrill-seeking thugs, nation-state hackers and internal staff or contractors. Research and real-world examples are showing a dramatic rise in attacks. In fact, Security magazine reported in 2014 that nearly 70 percent of critical infrastructure companies have suffered a security breach.

Securing an operational technology (OT) environment is significantly different than securing a traditional information technology (IT) environment. What you're securing is different, and how you secure it is different. IT focuses on digital information protection. OT focuses on people and physical asset protection. To deliver security solutions specific for OT requires an industrial mindset, purpose-built technology and specific OT security expertise.

There are immediate steps both device manufacturers and industrial operators can do to begin securing their most valued resources—people, environment and assets.

Assess – understand your vulnerabilities

Secure – install OT security solutions to secure critical assets

Certify – validate network robustness of industrial devices and confirm that they meet requirements

Security waits for no one. Get started today.

References

(Endnotes)

1 GE CEO Jeff Immelt: Let’s finally end the debate over whether we are in a tech bubble http://www.businessinsider.com/ceo-of-ge-lets-finally-end-the-debate-over-whether-we-are-in-a-tech-bubble-2015-12?utm_content=bufferd2f1a&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

2 GE Predix Software Platform Offers 20% Potential Increase in Performance, http://www.businesswire.com/news/home/20150929006773/en/GE-Predix-Software-Platform-Offers-20-Potential

3 http://www.gartner.com/newsroom/id/2905717

4 “Operational Technology Security – Focus on Securing Industrial Control and Automation Systems,” March 14, 2014, Earl Perkins: http://blogs.gartner.com/earl-perkins/2014/03/14/operational-technology-security-focus-on-securing-industrial-control-and-automation-systems/

5 SecurityWeek, September 17, 2015, “Russian Hackers Target Industrial Control Systems: US Intel Chief,” Eduard Kovacs: http://www.securityweek.com/russian-hackers-target-industrial-control-systems-us-intel-chief

6 Verizon 2015 Data Breach Investigations Report

7 CERT Insider Threat Center Blog, “Analyzing Insider Threat Data in the MERIT Database,” Matt Collins: https://insights.sei.cmu.edu/insider-threat/2013/10/-analyzing-insider-threat-data-in-the-merit-database.html

8 GE CEO Jeff Immelt: Let’s finally end the debate over whether we are in a tech bubble. http://www.businessinsider.com/ceo-of-ge-lets-finally-end-the-debate-over-whether-we-are-in-a-tech-bubble-2015-12?utm_content=bufferd2f1a&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

wurldtech
A GE Company

Wurldtech Security Technologies
Suite 2000, Four Bentall Centre
1055 Dunsmuir Street
PO Box 49133
Vancouver, BC V7X 1J1 Canada

T 1 877 369 6674
info@wurldtech.com
wurldtech.com