An eBook by Belcan, LLC

DEFENDING CRITICAL INFRASTRUCTURE

TACKLING THE REAL CYBER THREAT TO YOUR BUSINESS

“We no longer have things with computers embedded in them. We have computers with things attached to them.”

- Bruce Schneier

In 2014, a cyber attack made media headlines when a malicious email campaign nearly destroyed a German steel factory. Hackers with a deep understanding of industrial technology perpetrated a cyber attack against a German steel mill that brought virtual disruption into the physical world. The attack began as a breach of the corporate network and turned into a nightmarish disruption of critical infrastructure. Hackers used their illicit access to the office network as a jumping-off point to access the plant’s Industrial Control System (ICS). The attack compromised essential control components that resulted in plant-wide system failures.

The failure of the blast furnace’s control system is what made this attack so notable. With the necessary safety features disabled, the blast furnace commenced an improper shutdown. Blast furnace temperatures can exceed 4000°F, and malicious actors were able to unleash those potentially destructive conditions by compromising the plant’s ICS. The physical damage and loss of productivity that resulted were costly, but thankfully no one was hurt or killed.

The source of the breach? A targeted phishing campaign with a malicious email attachment.

Everyone agrees that data should be kept secure. While lost or compromised data is daunting enough, the possibility that industrial technologies can be compromised should be even more troubling. Operational Technology (OT)—a term that encompasses components that comprise critical infrastructure and affect the physical environment—might not seem like a viable target for a cyber attack, especially if legacy components are involved. There’s no serious risk when an old cooling unit is breached, after all. **Right?**

Wrong. Even if a component is “dumb” or predates Internet connectivity, it can still be vulnerable to destructive attacks. Seemingly “dumb” legacy components often communicate with other machines and control systems, sending data for monitoring and control purposes. The potential physical and economic damage caused by these systems when they fail or become uncontrollable is enormous.

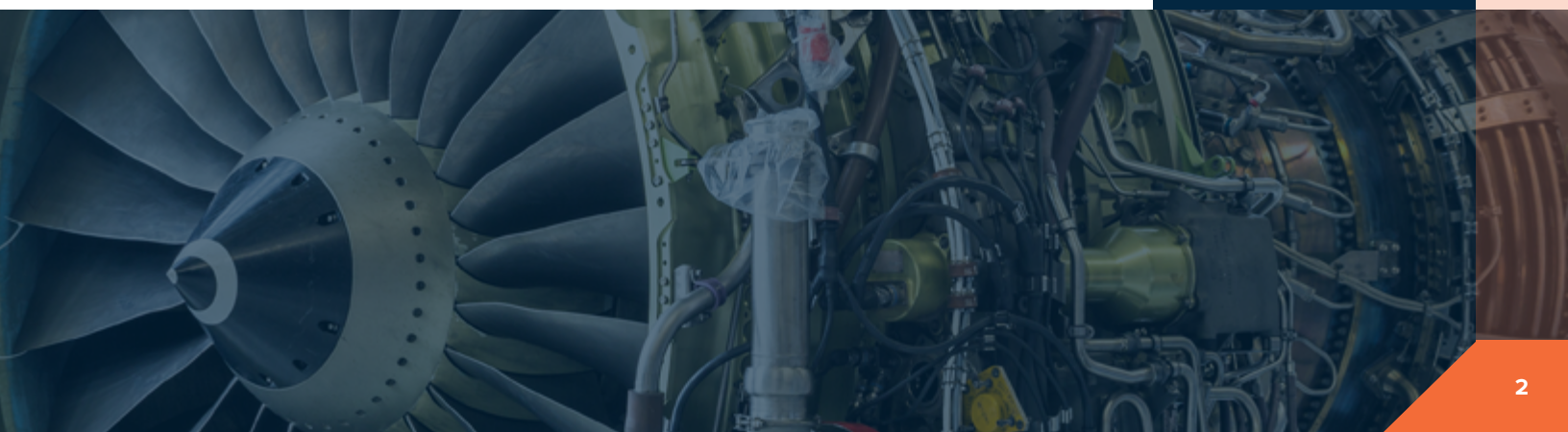
To remedy these security vulnerabilities, many organizations have turned to their IT departments and vendors, but IT expertise doesn’t necessarily translate to OT expertise. Your IT team might not know how to assess the risks facing your OT infrastructure, and your OT professionals might not know how to coordinate their security posture with other parts of the organization.

Security standards and federal compliance mandates for ICS and OT in various industries do exist, but properly implementing them may be challenging without the right resources and experience. And with the mix of legacy components and newer hyper-connected components common today, the situation becomes even more complicated. Whether your organization faces malicious actors or not, the visibility, safety and security of critical OT infrastructure in today’s mixed-connectivity industrial environments are crucial.

More than ever, organizations need an approach to OT security that accounts for the unique nature of these systems and their various components. One-size-fits-all security isn’t just inadequate—it’s unsafe. Organizations should take a holistic approach towards their digital hygiene to ensure the safety of their people and property in today’s changing risk environment.

Dumb Components: A device, sometimes analog or legacy, that lacks significant local compute and network connectivity.

Digital Hygiene: the discipline practiced to ensure the integrity and security of data.



IT and OT in the World of Industrial Internet of Things

Fifteen years ago, the domain of IT was well defined. IT departments handled the security and functionality of a finite number of machines within their organizations, making sure everything connected was safely tucked behind a fortress-like firewall. Wirelessly networked equipment was a non-issue, and employees didn't have to worry about digital hygiene on mobile devices. Phones had not yet become "smart." The physical plant would have been completely separate and largely self-contained. Where IT stopped and OT began was clear.

That's certainly not the case anymore. The Internet of Things (IoT) has torn down the wall and turned the IT ecosystem into a jungle. On the corporate side, everyone is connected through mobile devices, while peripherals like printers and scanners communicate wirelessly with their networks. Smart thermostats, doors, lights, and security put physical infrastructure onto the office network. IoT benefits have triggered adoption in other sectors, creating a new Industrial Internet of Things (IIoT). Connectivity is king. New machinery and components are born "smart," while older portions of the OT infrastructure may have been modified or augmented to speak to the ICS or Supervisory Control and Data Acquisition (SCADA) systems that monitor their performance, relay their data, and control their processes.

The divide between IT and OT teams presents a susceptibility for cyber risk to the organization. Vulnerability in the ecosystem creates an opportunity for not only malicious cyber criminals, but also accidental and negligent threats. Information silos and poor communication can result in a disjointed, unsafe approach to IT and OT security in the mixed-connectivity realm of IIoT. These risks are compounded by the lack of cross-domain knowledge between IT and OT sectors. That being said, it's important to understand the traditional differences between IT and OT:

IT, or Information Technology, manages connectivity and data at the enterprise level. An IT breach will affect an organization's intangible assets and may affect finances or disrupt productivity. IT vulnerabilities come from things like unsafe or unsecured Internet connectivity, user error, or poor authentication protocols. Enterprise email accounts, software updates, infected USB sticks or other insertable media, and poorly secured peripherals like printers and scanners are common sources of IT security breaches.

OT, or Operational Technology, manages physical processes and conditions. When breached, OT can pose a serious threat to physical property, productivity, human life, the environment, and to a nation's security. Breaches that target OT, such as SCADA systems, ICS, or machine-to-machine (M2M) communication, penetrate the system by gaining access to a connected IT network. The OT footprint of most organizations is varied, vast, and often obscure to the IT organization.

Organizations should capitalize on the different expertise and viewpoints of IT and OT professionals while paying attention to the need for collaboration and innovation in this new technological paradigm. We've seen a fundamental shift towards increased autonomy, information transparency, and connectivity to the cloud. Security measures need a sea change of their own to keep pace.

IT
• Data at rest / not real time data
• Cloud infrastructure, hardware and software
• Confidentiality focused
• Intended to store, process and deliver information
• Enterprise-wide
OT
• Data in motion / real time data
• Systems for monitoring and controlling
• Availability focused
• Legacy install base
• Purpose-built

Threats Facing OT Infrastructure

When you think of cybersecurity threats, your mind probably jumps to external malicious forces—teams of hooded hackers in dark rooms trying to access your data, for example—but the threats facing OT infrastructure vary widely. Ironically, the biggest threat to your organization might simply come from an aging, poorly maintained mix of components that aren't visible to your ICS. Knowing what kinds of threats exist can help organizations optimize their security.

The following types of threats pose risks to organizations today:

Aggressive Active Threats

Aggressive and active threats that actively target your organization with malicious code in order to compromise your systems or take away your control are frightening. Recent high-profile stories of costly ransomware attacks like WannaCry are certainly enough to strike fear in anyone's heart. But frequently, these aggressive threats rely on a path-of-least-resistance approach. With robust security and enterprise-wide awareness of digital hygiene best practices, the opportunity for bad actors to do harm is greatly reduced.

Aggressive Passive Threats

Hackers may not always seek to obtain access to your systems in order to disrupt service or damage your infrastructure. They may simply be placing a "listening ear" into your systems, either as a prelude to an active attack or as espionage. The same security measures that deter active threats can deter passive threats as well, but the low-key nature of their execution means that a successful passive attack may be undetectable, especially if your organization is poorly prepared.

Structural Threats

Your organization's OT footprint might be an invisible threat. A component's age, and different layers of updates and modifications can create problems like lack of visibility or vulnerability to exploitation. Changes to the OT footprint can also disrupt your security posture. A lack of system visibility due to structural issues can be just as dangerous as something perpetrated by a malicious actor.

Insider Threats

Sometimes the threat to your organization sits in a desk down the hall. Malicious insiders (disgruntled or unethical employees), ingenious insiders (employees or administrators who make changes to your OT environment to make their jobs easier), or careless insiders (who click on links in phishing emails or conduct themselves riskily on company networks) can pose a major threat to any organization. Educating all employees on proper digital hygiene and creating reliable forms of access control should help mitigate this risk.

3-Step Approach to OT Security

Belcan's comprehensive 3-step approach to enhancing OT security is designed to address the issues facing a wide range of organizations—whether your footprint is heavily comprised of legacy parts or if you're on the cutting edge of the newest industrial technology.

1

Assess

Know where you are. Belcan gives you a full picture of your entire OT footprint and provides services like vulnerability testing, penetration testing, ethical hacking, and technical and process assessment.

2

Remediate

Get where you should be. Belcan uses its deep reservoir of subject-matter expertise to address vulnerabilities, oversights, and gaps in training. Get increased visibility of system processes and improve your system's hygiene.

3

Sustain

Stay ahead of potential threats. Belcan leverages threat intelligence and continuous monitoring to prevent issues before they emerge. Continued management of your data allows Belcan to model the impact of hypothetical events and develop remediation strategies to face them head on.

Belcan's IT Command Center can provide 24/7 technical support across the whole lifecycle of this domain, freeing up valuable IT resources.

5 Things to Take Control of Today!

1. Take inventory of your hardware.

Simply knowing where your systems are, what they are, and how they communicate with each other can go a long way towards eliminating blind spots in your OT infrastructure.

2. Take inventory of your software.

If you're running an unsupported OS or other defunct software in your organization, you're opening yourself up to potential breaches. Find out what software you're relying on. Measure the OT (legacy systems) lag behind manufacturer's recommendations.

3. Examine your configuration.

Determine whether your systems are configured for security—not convenience. Utilizing configuration standards like the CIS Benchmarks can harden your systems and prevent users from accessing critical functions at the OS level.

4. Evaluate your vulnerability scanning & remediation protocols.

Have all of your systems received security patches? Do you have a comprehensive patch management system? Promptly installing updates and assessing system vulnerabilities on an ongoing basis can head off breaches.

5. Consider controlling the use of administrator privileges.

Users should only have the rights and privileges they need to do their jobs—period. Don't over-share administrative privileges. Be sure that users and administrators have appropriate permissions for daily tasks to head off problems, whether intentional or accidental.

Belcan

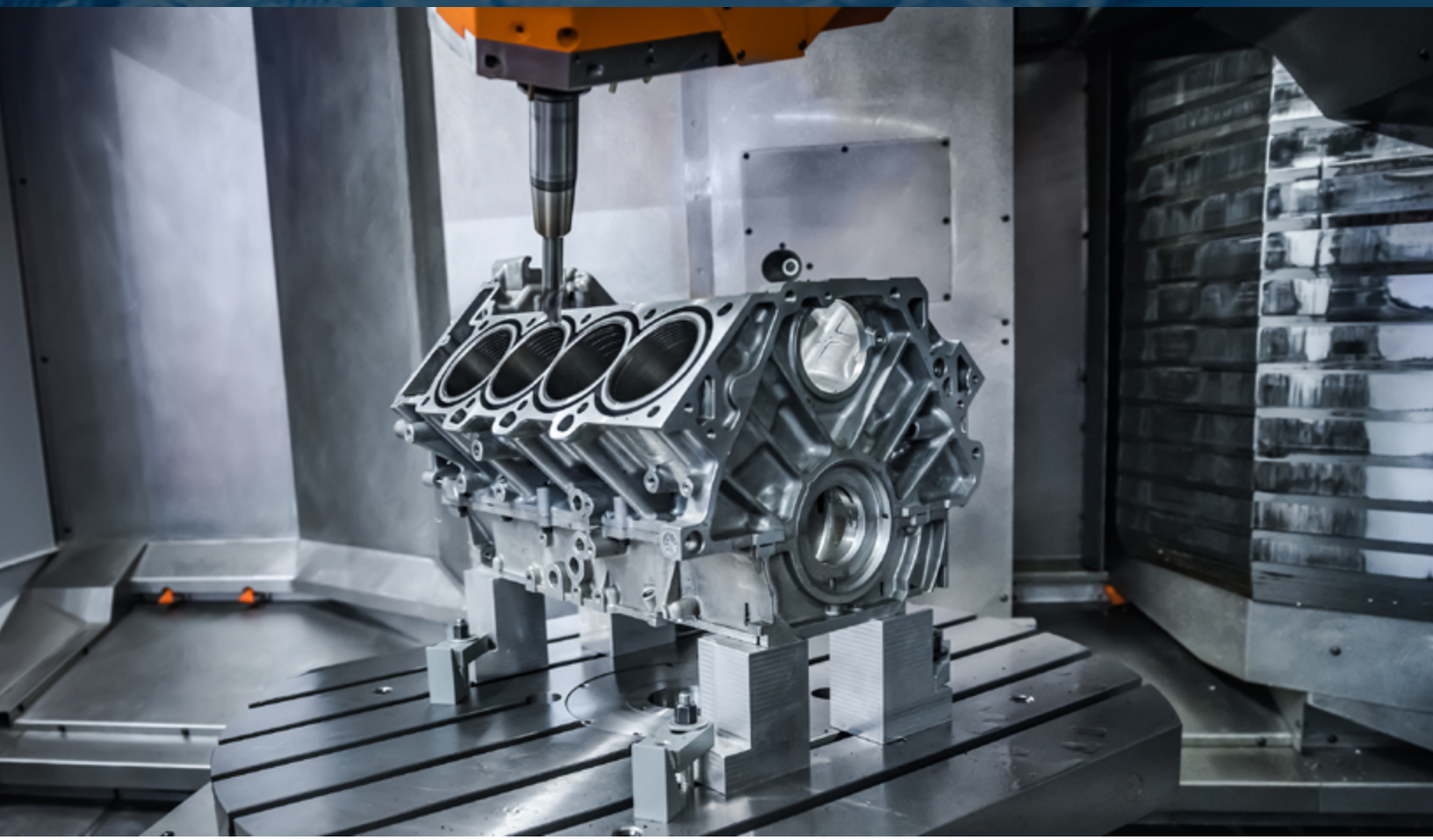
When OT security is mission critical, it's not a "nice to have" anymore.

Why Partner with Us?

Belcan has decades of experience in this domain designing, supporting, and protecting industrial data. For Belcan, securing critical OT infrastructure will never be an afterthought. We draw from a deep pool of talent, bringing in experts to minimize the burden on your staff. That means no more choosing between mission-critical tasks and pursuing operational hygiene. Belcan teams possess the techniques and domain expertise needed to deliver professional assessment, remediation, and ongoing sustainment for this threat landscape.

Belcan's subject-matter expertise means confidence—the confidence of a comprehensive approach to this crucial aspect of your organization.

GLOSSARY OF TERMS



Digital Hygiene	The discipline practiced to ensure the integrity and security of data.
Line Replacement Unit (LRU)	An LRU is a modular component of a vehicle, such as a ship or aircraft, that allows easy replacement for maintenance and upgrade activities.
Ransomware Attack	A cyber attack that involves denying a person or organization access to components or data until a ransom fee is paid. Most notably, a corporation's data is encrypted on the corporation's own storage devices, making it unreadable until the fee is paid.
Cyber Attack	Any attack that targets an organization's communications network, computer systems, or other connected components.
Breach	A specific event denoting an incursion into a computer system or communications network.
Smart devices	A device or component that has local compute and/or network connectivity.
Dumb devices	A device, sometimes analog or legacy, that lacks significant local compute and network connectivity.
Information Technology (IT)	The devices, components and policies that are used to support an enterprise, typically back-office focused and managed by a CIO.
Operational technology (OT)	Hardware, software, and policies that impact the reporting and/or operation of devices and processes critical to line of business activities. Often run by LoB management and Operations.
SCADA	Supervisory Control and Data Acquisition is the term for a common architecture used to control industrial devices and systems, typically used in Manufacturing and Utility industries.
Machine-to-Machine (M2M)	Describes communications between devices. There is no explicit medium, architecture, or protocol for these communications, but it is typically used describe ICS communications.

Clint Green | clintgreen@belcan.com

Vice President, Technology & Innovation | Belcan Government Services (BGS)

Clint's background includes over 20 years in the technology industry. Clint has supported various companies ranging from OEMs to Large Services Integrators (LSIs) to start-ups. In these roles, he has always provided guidance and input into advancing the solutions and technology he was supporting. As a forward thinker, he understands complex problems and solutions, often being relied upon by customers and senior leaders to design advanced solutions

About the Authors

Michael Baisden | mbaisden@belcan.com

Cyber Security Solutions Manager, Belcan Government Services (BGS)

Michael Baisden has over 20 years of cyber security, information technology, and training experience in both government and private sector. As Belcan's expert in cyber security solutions, Michael provides the technical and programmatic expertise for the implementation of effective and sustainable cyber security programs in various sectors. Michael is a Certified Information System Security Professional (CISSP) and Certified Information Security Manager (CISM).

About Belcan

Belcan is a global supplier of engineering, technical recruiting, and IT services to customers in the aerospace, defense, industrial, and government sectors. Belcan engineers better outcomes through adaptive and integrated services. From jet engines, airframe, and avionics to heavy vehicles, chemical processing, and cybersecurity, Belcan takes a partnering approach to provide customer-driven solutions that are flexible, scalable, and cost-effective. Belcan's unique capabilities have led to continuous growth and success for nearly 60 years. For more information, please visit www.belcan.com |

“There are only two types of companies:
those that have been hacked,
and those that will be.”

- Robert Mueller -
FBI Director, 2012