— Engineering Better Outcomes

Belcan

Staying Ahead of OT Cyber Risks

Increasing Government Emphasis on Cyber Resilience

Recently, the UK government announced plans to introduce new laws to strengthen national resilience to cyber attacks.[1] Consultation has started on amending the 2018 Network and Information Systems (NIS) regulations in response to growing threats and a number of recent high-profile cyber incidents, including threats to critical national infrastructure. The Minister of State for Media, Data, and Digital Infrastructure, Julia Lopez, stated that taking cyber resilience seriously is "not an optional extra."

Overlooked Vulnerabilities

Research conducted by the Department for Digital, Culture, Media and Sport in 2021 revealed widespread and persistent cyber security vulnerabilities in UK organizations, especially regarding supply chain-related threats[2]:

> **Only 12 per cent** of organisations review the cyber security risks coming from their immediate suppliers.

> **Only one in twenty** (5 per cent) address the cyber security vulnerabilities in their wider supply chain.

Individuals and organizations alike are familiar with common cyber risks that have become part of everyday life: from attacks as simple as phishing emails to ransomware attacks that endanger private information and incur steep costs. What are less familiar are the vulnerabilities of our Operational Technology (OT); the hardware and software systems that monitor and control industrial processes, devices, and infrastructure within industries such as manufacturing, energy generation and distribution, aerospace, and rail.

Whilst IT cyber incidents tend to target data for exploitative purposes, attacks on OT attempt to gain a level of control over a physical operation or production facility, typically with the intention of disrupting operations. This could entail anything from reducing efficiency and productivity, to denial of service, to catastrophic failures that risk environmental emissions, stock, and personnel:

Dangers Posed by OT Cyber Attacks

In 2015, the control systems of a German steelworks were breached via malicious code embedded in emails, allowing hackers to interfere with the shutdown of a blast furnace, which suffered catastrophic damage.[3]

In 2017, malware named Triton was discovered at a Saudi Arabian petrochemical plant, designed specifically to take control of remote safety workstations. The intrusion was thwarted before damage could be done.[4]

In 2020, hackers gained access to Israeli water treatment facilities in order to alter chlorine levels. This attack was detected and halted before attackers were able to poison the population.[5]

Challenges Securing OT Infrastructure

The emergence of the Industrial Internet of Things (IIOT), coupled with the connectivity demands induced by the Net-Zero transition and evolving requirements for optimisation and data driven processes, is impacting how facilities operate across sectors. Manufacturing, transport, chemical, pharmaceutical and critical infrastructure facilities are pushing towards remote processes, unmanned remote stations, and OT/IT systems integration. These rapid advances are expanding a significant, frequently unacknowledged attack surface and widening the industrial cyber security gap.

A key challenge in securing OT infrastructure is knowing where to start, especially taking into consideration the large volume of assets and complex connectivity inherent to most systems. State of the art IT security relies heavily on rapid updates and reactionary patch management, with modern weekly or daily update cycles. This is in stark contrast with current OT systems, where security patching OT components often requires complete shutdowns. The process of hardening OT systems against cyber attack can result in halted production, long downtimes for integrated manufacturing systems, or even disruption of bespoke software, validation, and verifications systems—especially without dedicated mitigation measures in place.

Security Challenges – IT vs. OT

IT			OT		
Attackers typically target sensitive data to steal or ransom	Security depends largely on rapid, continuous updates/patches to softwarem	Weekly/daily update cycles; minimal impact to operations	Attackers target industrial control systems (ICS) and facilities to gain control or disable	Security requires a holistic approach to securing systems and organization processes	Lengthy update cycles; potential for significant impact on operations

Amongst other constraints, the rapid patch/release cadence accepted within IT environments simply cannot be deployed within current OT environments, requiring an OT-specific approach to risk identification, mitigation, and security integration with existing organisational processes. It used to be common for organizations to rely on air-gapping and islanding for protection of OT systems, but even islanded systems are at risk. Disgruntled employees, the growing threat of supply chain attack, and physical site penetration are equally significant risks to consider. Service engineers with infected laptops or bad actors seeking employment can all bring plants to a complete shutdown and cause catastrophic failure.

Progressively Mitigating Risks

Through the deployment of effective isolation, segmentation, and least-functionality-driven security architectures, the impact of vulnerabilities and IT-driven constraints can be mitigated. Combining these measures with procedural and human factors can further drive systematic change and enhancement to OT cyber resilience.

An intentional approach to securing OT should start with a clear understanding and definition of the system's vulnerabilities. Belcan has adopted a structured approach that begins with developing a map of connected assets and leveraging cyber threat attack path modelling to identify the initial priority areas, which generates clear, actionable results. Our verified threat model can then produce a report that allows asset owners to justify expenditures against an often-limited security budget. The report also provides board-level or executive decision makers with validated figures to influence endorsement.

The Belcan Approach

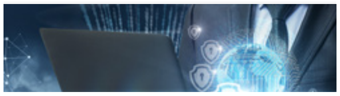
1

Fully map interconnected OT systems

2

Model cyber threat attack path to understand vulnerabilities

3



Generate a report with clear action items to justify spend

Achieving a Stronger Security Posture with Belcan Expertise

At Belcan, we focus on OT networks and operations by designing cyber security solutions with demonstrated compliance against the NIS Directive, the IEC 62443 standard, and NIST and NCSC guidelines from the ground up. Our standards-based approach ensures OT cyber requirements are "front and centre" in terms of functionality and maintainability. Instead of replacing entire systems, Belcan's OT specialists and cyber security experts are experienced in working with asset operators and owners to address their existing systems by identifying weaknesses, reviewing risks, and strengthening resilience through configuration techniques that reduce the attack surface for OT systems. Adoption of – and strict adherence to – rigid operational policies and procedures is often the first consideration in our reviews of existing systems. Cost efficient solutions like this, combined with effective risk analysis, security-driven architecture, and segmented deployment, will augment OT cyber resilience within industrial processes and operations.

Belcan's proven OT expertise and cyber security solutions are provided across high-risk critical national infrastructure sites, energy, utilities, and manufacturing, enabling clients to achieve cyber security compliance through bespoke design, assessment, and solution delivery.

To find out more on how Belcan can help enhance your OT cyber security:

Contact Us

Belcan

References

[1] Press Release: New laws proposed to strengthen the UK's resilience from cyber attack. https://www.gov.uk/government/news/new-laws-proposed-to-strengthen-the-uks-resilience-from-cyber-attack

[2] Press release: Businesses urged to act as two in five UK firms experience cyber attacks in the last year. https://www.gov.uk/government/news/businesses-urged-to-act-as-two-in-five-uk-firms-experience-cyber-attacks-in-the-last-year

[3] "Hack attack causes 'massive damage' at steel works." https://www.bbc.com/news/technology-30575104

[4] "Triton: hackers take out safety systems in 'watershed' attack on energy plant." https://www.theguardian.com/technology/2017/dec/15/triton-hackers-malware-attack-safety-systems-energy-plant

[5] "Two more cyber-attacks hit Israel's water system." https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/