Bridewell

Cyber Security. Where it Matters.

Operational Technology
Cyber Security Services

Contents

The Importance of Securing Operational Technology

Operational technologies are computer-based systems that interact with the physical world, and are typically used to provide automation, remote visibility, and control of physical processes. OT environments present unique security challenges that require specific experience and skillsets to be addressed appropriately.

- **OT and Cloud** – The use of the cloud for OT applications is still in its infancy, and the reliance upon third-party hosting and network services to deliver critical OT services is a concern for most operators.

- **Unique Governance Stack** – Organisations with OT environments are typically subject to frameworks and regulator guidance such as the Cyber Assessment Framework (CAF), OG86, and ISA/IEC 62443.

- **Security Architecture** – Poorly secured pathways in your security architecture can expose your critical systems to cyber threats. Simple controls assessments don't always reveal open attack vectors, and a more holistic analysis of the security architecture is required.

End-to-End Cyber Security Services for OT

How OT is used within an organisation will vary significantly, depending on their specific applications, vendors, heritage of equipment, external integration/connectivity and cyber security maturity. While we see synergies across the clients we work with, this often makes for a unique set of challenges to be addressed.

With a complete suite of cyber security services for OT that can be tailored to your specific needs, we can support from assessing your environment through to establishing a security model or running your estate. At the core of every OT engagement are one or more of our specialist OT cyber security consultants. Where additional specialisms are needed, we will also draw upon the full breadth of expertise across Bridewell to provide a multi-disciplined team of experts.

Understand

Gain Deep Insights Into Your Cyber Security and Resilience

OT Security Posture Assessment

This is our base level assessment that maps out your environment and current security controls, allowing us to identify areas of significant weakness that may expose systems to threats. This is suited to all environments to give a solid foundational analysis, but is especially valuable for systems where there is limited understanding of the security posture or where information is considered out of date.

A security posture assessment allows us to map out the environment and current security controls in place. This approach is useful for organisations who have limited knowledge of their environment and wish to understand:

- Areas of immediate concern that need improvement.
- Opportunities for security enhancements to be made.

Areas covered by the assessment:

- **Key Asset Types**
  Main hardware and software components in operation across the environment.
- **System Data**
  Data produced and consumed by the system, the criticality of this data, and pathways used to transmit and receive data.
- **Network Architecture & Segregation**
  Assets are segregated from one another at the network level and the controls in place to govern inter-network comms; both internally and with external networks.
- **Identify and Access Management**
  Authentication and authorisation mechanisms for system access.
- **Network Access Control**
  Controls protecting against the connection of unauthorised devices.
- **Remote Access**
  Mechanisms in place to allow users to access systems from external networks, and how are these secured.
- **Vulnerability Management**
  Vulnerability discovery and remediation mechanisms.
- **Malware Protection**
  Controls in place to protect against the ingress and/or execution of malware.
- **Backup**
  System back up mechanisms, and how backups are controlled and tested.

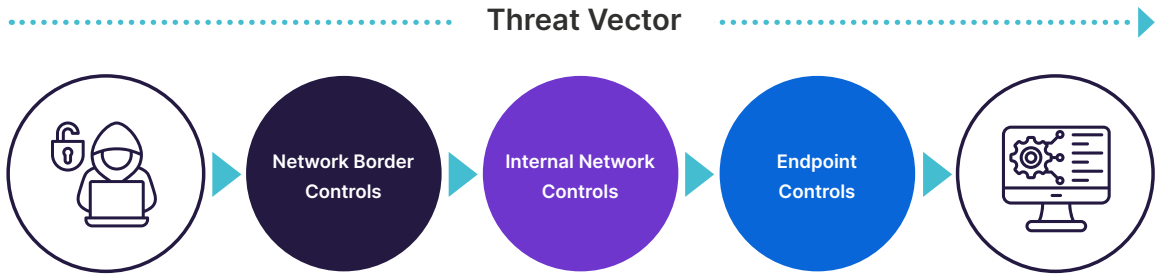
Output

You will receive a detailed report covering the areas assessed, including a system and network topology providing a graphical representation of the arrangement and interconnection of various elements making up the environment. Across all areas we will detail strengths and weaknesses, with recommended improvements to enhance the security posture.

Threat Modelled Risk Assessment

Cyber risk assessments often attempt to analyse the risk posed by individual control deficiencies. This may give an inaccurate view if not considered in the wider context of a defence-in-depth architecture. We map out the pathways across the environment that could be exploited by threats, assessing the controls in operation along each pathway to determine the level of threat exposure. This allows us to assess the risk of cyber attack rather than focusing on individual control deficiencies.

Where an OT Security Posture Assessment has been recently performed, we use this as the basis of the risk assessment to deliver efficiency in the service.



Framework Gap Analysis

Bridewell has extensive expertise in most common cyber security frameworks used within OT environments. We perform detailed gap analysis against these frameworks to identify areas where improvements are needed to meet requirements. We contextualise any gaps found, allowing us to provide targeted recommendations for remediation tailored to your specific environment. Frameworks we commonly work with include:

General Frameworks

- NCSC Cyber Assessment Framework (CAF)
- CAA ASSURE Scheme/ CAF for Aviation
- ISA/IEC 62443
- NIST Cyber Security Framework (v1/v2)
- NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security
- IEEE 1402-2000 – Guide for Electric Power Substation Physical and Electronic Security
- IEC 62351 – Power Systems Management and associated Information Exchange
- Secure PLC Coding Practices: Top 20 List

Safety Specific Frameworks

- ISA-TR84 – Security Countermeasures Related to Safety Instrumented Systems
- IEC 61508 Functional Safety Standard
- IEC 61511 Functional safety – Safety instrumented systems for the process industry sector
- HSE OG86 Cyber Security for Industrial Automation and Control Systems (IACS)

Asset and Vulnerability Discovery

The accuracy and completeness of OT asset data may be called into question if it has not been regularly maintained. This in turn can hamper the ability to maintain an up-to-date understanding of the presence of firmware vulnerabilities across the environment. We have a range of techniques that can be adopted to discover assets and vulnerabilities within any given environment, often without the need for additional specialised tooling.

OT Asset Discovery Sources

- System documentation
- SCADA systems
- MAC address tables
- Packet captures
- OT configuration tools

Vulnerability Identification Methods

- Firmware version lookup against public or private vendor vulnerability databases.
- Monitor vendor vulnerability notifications, comparing the firmware of affected version against firmware versions in use.

Threat Intelligence

Staying informed of new emerging threats allows you to keep ahead of the risk they may pose to your systems. By leveraging sector-specific intelligence and real-time data analysis, our team delivers tailored threat insights and actionable recommendations that enhance detection and response capabilities for each client.

- Improve quality of risk evaluation
- Inform decision making to guide your security program
- Take pre-emptive countermeasures in response to new emerging threats

Download the Report:

Advise and Mandate

Establish Your Security Model

Foundations for Mature Security

Security Advisory

Bridewell's OT technical specialists are on hand to provide expert advice and guidance on any area of OT cyber security. We have previously delivered this service through a range of mechanisms, from workshops and presentations through to embedding people with the company's operational or project teams. Specific services we offer to mature your cyber security capabilities, include:

OT Security Strategy

A cyber security strategy sets out the core goals and objectives that need to be achieved. We work with your senior stakeholders to develop your OT strategy to meet operational needs, achieve regulatory compliance, address current cyber security challenges, and keep protected against new emerging threats.

OT Policy and Process

We build your policy framework as either a standalone set, explicitly for your OT environment, or fully integrated with wider business cyber security policies. We bolster policies with a set of structured processes to provide efficient and consistent delivery of policy requirements.

Target Operating Model

A target operating model defines the business structure, roles, competencies and resource levels to deliver and operate effective cyber security. Aligned to your specific needs, we can define comprehensive models to cover your entire operation, or focus on individual areas where, for example, new security capabilities are being introduced.

Training and Awareness

Training and awareness on any aspects of OT cyber security from our OT technical specialists. Delivered as standalone sessions or integrated into wider business training and awareness initiatives.

Implementing OT Frameworks

Operators of OT systems will encounter a variety of security frameworks and regulator guidance specifically designed for industrial environments. Navigating these frameworks can be complex, requiring expertise in cyber security, OT systems, and industrial processes.

Bridewell's OT security technical specialists have significant experience in implementing numerous security and safety frameworks across diverse industrial settings. Their expertise enables them to provide informed guidance on the most effective approaches to meeting the requirements of these frameworks, ensuring robust protection for critical OT environments.

ISA/IEC 62443

The ISA/IEC 62443 series of standards define a range of controls and processes designed specifically for the electronic security of industrial automation and control systems (IACS).

Bridewell's OT specialists are not only certified against these standards but are also active contributors to their ongoing upkeep and development. We deliver a full range of services against the framework to support its implementation within your environment.

Cyber Security for Safety Critical Systems Advisory

Bridewell's OT security specialists provide expert advice and tailored guidance specifically for systems operating within safety-critical environments.

With a TÜV Rheinland Functional Safety Engineer as part of our team, we are uniquely positioned to deliver comprehensive cyber security advisory services aligned with a broad spectrum of safety standards. Our in-depth knowledge ensures that your OT systems not only meet regulatory requirements but also achieve the highest levels of protection and operational resilience.

Develop

Define Measures to Protect, Detect and Respond to Cyber Events

Develop Robust Defences

Risk Remediation and Improvements Plans

Building upon our assessment services, we define security measures to address identified deficiencies and risks, and improve the overall security posture. These are developed into a prioritised roadmap which sequences implementation steps according to their criticality and feasibility, accompanied with a comprehensive set of plans for delivery.

Cyber Informed Engineering

Cyber-Informed Engineering (CIE) is a proactive approach that integrates cyber security considerations into the design, development, and operation of physical systems—especially those in critical infrastructure like energy, water, and transportation. Rather than treating cyber security as an afterthought, CIE embeds it from the earliest stages of engineering. This allows engineers to “engineer out” cyber risks before systems are built, making defenses more effective and cost-efficient.

Security Architecture Design

Work with our blended teams of security architects and OT technical specialists to design secure and resilient inter-connected OT architectures and solutions, whilst minimising threat vectors. We deliver high and low-level designs detailing system and network architectures, and the specification of security controls and configuration. This is accompanied by a full set of security requirements for action by the delivery team.

Remote Access

Remote access presents the most significant initial access vector for threats seeking to target OT systems. Develop secure remote access for your OT estate, with solutions ranging from VPN deployments to sophisticated zero-trust models.

Reference Architectures

Reference architectures accelerate delivery whilst maintaining consistency in system designs. Our specialists develop libraries of modular reference architectures to meet the specific needs of your environment. Modules are designed to be combined into holistic platforms that deliver commonality whist also meeting security compliance requirements.

Develop Detection and Response Capabilities

Security Event Collection

Sources of security event data in OT environments may be scarce and extraction to management platforms such as SIEM difficult to achieve.

Bridewell has extensive experience with this challenge and has developed several methods to obtain essential data for effective security monitoring. Through our service, we identify sources of event data, options for deploying tooling for further coverage, and mechanisms to extract data without introducing additional vectors for attack.

Threat Response Plans

Having pre-defined plans to respond rapidly to indicators of threat can prevent exploit, infection, and harm to systems.

Threat response plans define the inter-relationships between systems, the minimum connectivity required to maintain essential operations, how to enact this mode, and aspects to be considered taken prior, during and after enactment.

Incident Response Plans

Having an effective means to respond to a cyber incident is vital to minimise impact to critical operations. We develop and mature your processes, procedures and playbooks, then verify their effectiveness with the support of the Bridewell Incident Response team.

Deliver

Delivery of Security Infrastructure

Operational Technology Cyber Security Services

Security Infrastructure

OT Cloud Platforms

There are many non-mission critical aspects of OT that can only be successfully delivered in the cloud (e.g., storage of historic data, hosting of security management services, and delivery of remote access systems). The use of hybrid cloud is also an exciting opportunity to allow the delivery of mission-critical OT services. Bridewell is ideally placed to support operators of essential OT services in navigating this landscape, due to the expertise and firsthand experience held within our OT function and Security Architecture team.

Firewall Solutions

As one of the most important initial access and lateral movement protection controls, operating securely configured firewalls is a vital defense to protect against the ingress of threats. We deliver resilient firewall architectures and robust firewall rule sets into complex environments, to implement perimeter security and internal segregation controls.

OT Security Sensors

OT security sensors that provide asset and vulnerability discovery and threat detection can be valuable tools to compliment your security infrastructure. If not utilised correctly, however, you are unlikely to obtain the full benefits of these products. With experience across multiple vendors and combining our deep expertise in OT control systems, protocols and networking, we can ensure security sensors are delivered to achieve maximum benefit within your specific environment.

Operate

Run Your Estate With Managed Security Services

Managed Security Services

Vulnerability Management

Our Vulnerability Management as a Service (VMaaS) provides end-to-end management of technical security weaknesses in your OT estate. We identify, analyse, and track vulnerabilities, working closely with your internal teams to ensure effective remediation. With ongoing monitoring, coordination, and reporting, we help reduce risks and strengthen your OT security posture.

Security Monitoring (SOC)

Defend your organisation against cyber threats and gain access to a range of leading SOC services, supported by industry leading security analysts and cyber threat intelligence.

Threat Response

In the face of new or heightened threats, implementation of temporary security measures to protect your OT systems may be required until the threat has passed or been neutralised. Rapid response is vital to ensure these measures can be implemented before the threat causes harm. This is aided by understanding the services and connections that can be temporarily halted whilst still maintaining operations to prevent the ingress of threats.

Digital Forensics and Incident Response

Our SLA-backed incident response services, for either retained or emergency incident response, gives you 24/7 access to our digital forensic incident response (DFIR) professionals. Our DFIR team will be on call 24/7 to respond to a security incident, providing digital forensics with chain of custody for evidence that can be trusted for use in legal or civil proceedings and/or litigation.

Assure

Validate Your Security Measures and Identify Opportunities for Further Improvement

Security Measures Validation and Improvement Opportunities

Program Assurance

Complex cyber transformation programs require oversight by cyber security specialists to ensure all requirements are fully achieved to meet compliance and security objectives. Whether it's an OT focused program or a business wide program incorporating OT, we build teams covering all applicable domains, to assure successful program delivery.

Offensive Security Simulation

Simulating offensive attack techniques is essential for gaining confidence in the ability for a system's security countermeasures to repel threats. All our engagements are tailored to provide a realistic simulation of how bad actors may target your organisation. Our penetration testing services have been developed to help CNI organisations identify, test and secure their most critical OT systems, whilst avoiding harm to the operation of devices that may be sensitive to certain techniques.

OS Build Assurance

OT environments often rely on servers and workstations to run essential services such as SCADA. Hardening the OS, patching vulnerabilities, and running endpoint protection controls limits system attack surface to minimise exposure to threats. Delivering these measures in OT environments may be challenging due to limitations such as operating conditions, age of systems, or requirements of OT applications. We provide design and delivery assurance, to verify that systems have been developed to provide optimal security considering their operating context, and an independent analysis that all design requirements have been successfully delivered prior to go-live. For systems in service, we provide periodic build reviews to ensure systems maintain a robust security posture for the duration of their lifespan.

Network Security Assurance

Network security is an essential component of any cyber security strategy, but especially in OT where the ability to apply security controls at the device level may be limited. Our design assurance adopts the concept of zones and conduits defined by ISA/IEC 62443. We validate that networks have been segmented to group assets with commensurate security characteristics, and that firewalls governing data conduits between these zones explicitly control communications to specific hosts and services. Ongoing assurance of firewall rules is also critical, as overly permissive rules can creep in, leading to ineffective segregation.

IDAM Assurance

Limiting system access to robustly authenticated users, with the minimum access rights to perform their duties, is an essential defence in protecting against unauthorised access. Our IDAM assurance service is two-fold. Firstly, to assure the technical infrastructure is operating robust authentication protocols, enforcing reliable authentication factors. Secondly, we assure your JML procedures are being correctly followed to register and de-register users promptly and achieve principles of least privilege.

Incident Response Exercises

Rehearsing response plans enhances your preparedness for real-life incidents. We can run incident response exercises to any given cyber security scenario, either with our standard material that covers standard scenarios, or by developing customised content to meet more specialised events.

Key Research Findings for CNI Organisations in 2025

Key Research Findings for CNI Organisations in 2025

The top challenges facing CNI organisations are consistent with last year – mainly being data privacy, cyber resilience and cloud security. Confidence in cyber security has increased slightly, as has levels of outsourcing for cyber security and managed security services.

Research shows incident response times are still slower than needed, with 69% of CNI organisations taking up to six hours to respond to ransomware. Although there have been minor improvements, delays over an hour remain a serious concern and increase the risk of severe impact from ransomware attacks.

Download the Report:

Source: Cyber Security in Critical National Infrastructure 2025 Research Report

Our Certifications, Accreditations, and Awards

We currently offer more NCSC assured services than any other company. Below are all of our certifications, accreditations and awards.

Testimonials

"We had the technical capabilities to do this on our own, but we wanted to work with a company that had been there and done that. We knew that Bridewell had the relevant experience in aviation as well as ASSURE accreditation so could avoid the pitfalls and complications which can arise in this sector."

Tony Johnson, Head of Cyber Security Operations,Manchester Airport Group

MAG Manchester Airport

nadara

"We have been most impressed with Bridewell's proactive approach to security. When we discover information about attacks in our industry or hear of attacks elsewhere to which we may potentially be vulnerable, they are able to respond quickly and effectively."

Chris Lawrence, Group IT Security Manager, Nadara

Our Journey

2013

- Bridewell LLP formed and established as a cyber security consultancy

2014

- ISO 27001 Certified

2015

- Bridewell Consulting presented on the challenges of Big Data and Security at the ISC2 Security Congress in Munich

2016

- Portfolio diversified to include data privacy, penetration testing and managed security services
- NCSC Certified

2017

- New office opened in Newport

2018

- New office opened in London
- CREST accredited for penetration testing
- Changed from LLP to Ltd

2019

- Achieved Investors in People Silver accreditation
- 24/7 Security Operations Centre (SOC) opened in Newport
- ISO 9001 Certified
- Ended year with 27 employees

2020

- Achieved ASSURE accreditation from the Civil Aviation Authority (CAA)
- IASME accredited
- Named in global prestigious CyberTech100
- Achieved QSA Status for EMEA from the Payment Card Industry Security Standards Council (PCI SSC)
- Achieved Microsoft Gold Partner status for Security and Azure Cloud competency
- Ended year with 50 employees

2021

- Secured multi-million investment from Growth Capital Partners
- Joined the Microsoft Intelligent Security Association
- CREST accredited for SOC services
- Opened 5 new UK regional offices
- Doubled in size despite the pandemic
- Became carbon negative
- Won Cyber Business of the Year 2021 at The National Cyber Awards
- Won Tech Company of the Year and SME 100 Growth (under £10m) at the Thames Valley SME 100 Growth Awards
- Ended year with 141 employees

2022

- Won Santander Growing Business of the Year Award
- Won Cyber Security Excellence Award
- Opened US Office in Houston, Texas
- Achieved SOC2 accreditation
- Rebranded to Bridewell
- Opened new SOC in Cardiff
- Ended year with 191 employees

2023

- Won Cyber Security Company of the Year at the Thames Valley Tech Awards
- Won Workforce of the Year (2023) at the Thames Valley SME 100 Growth Awards
- Featured as MISA Finalists – Security Services Innovator
- Accredited for: CIR Level Two (NCSC), CHECK Penetration Testing, CREST CSIR, and SOC2
- Achieved Microsoft Verified Managed XDR Solution Status

2024

- Acquired public sector cyber security specialists, Arculus Cyber Security.
- Achieved Investors in People Gold accreditation
- Joined Microsoft Copilot for Security Partner Private Preview
- Hosted First CNI Cyber Security Summit
- Cyber Business of the Year Award Winner at The National Cyber Awards
- Assured Service Provider for the Cyber Resilience Audit scheme
- Finalist in The Growing Business Awards
- Named Among Fasted Growing Firms in the UK Fast Growth Index 2024

2025

- Strategic partnership announced with leading French MSSP, I-Tracing
- Recognised by Microsoft Security Excellence Awards as an Endpoint Management Trailblazer Finalist
- Won Cyber Security Services Provider of the Year at the 2025 Cyber Security Awards
- Bridewell Earns Information Protection and Governance (IGP) Security Specialisation
- Bridewell Named One of the UK's Best Workplaces for Development™ 2025
- Bridewell Named One of the UK's Best Workplaces for Wellbeing™ 2025
- Bridewell Named One of the UK's Best Workplaces for Women™ 2025
- Recognised with the Defence Employer Recognition Scheme Gold Award for outstanding support to the armed forces community.

Our Office Locations

Reading (Head Office)
Thames Tower
Station Road
Reading
RG1 1LX

London
5 Merchant Square
London
W2 1AY

Cardiff
Churchill House
Floor 7
Cardiff
CF10 2TW

Manchester
111 Piccadilly
Manchester
M1 2HY

Edinburgh
Forth House
28 Rutland Square
Edinburgh
EH1 2BW

Houston, Texas
800 Town & Country Boulevard,
Suite 500,
Houston,
Texas
77024

New York
12 East 49th Street
New York
NY 10017

The Bridewell Difference

Trusted and Recognised Across Industries

Highly Accredited
Certifications including: NCSC, CREST, ASSURE, IASME, Cyber Essentials Plus, ISO 27001, ISO 9001 and PCI DSS.

Trusted by Microsoft
Recognised as a leading worldwide security partner by CEO Satya Nadella at Microsoft Inspire.

Award Winning
Award winners at the Growing Business Awards 2022 and The Cyber Security Excellence Awards 2022.

Customer-centric Services

Customer-First All the Way
Bespoke services that deliver guaranteed outcomes, business impact and positive change.

An Extension of Your Team
Working with you, not for you, as if we were part of your own in-house team.

Agile, Responsive Delivery
Use automation and integration to drive real value and deliver efficiencies where possible.

Supporting the Cyber Community and Beyond

Developing Cyber Skills for the Future
As an NCSC partner, we support UK schools, colleges and universities to encourage and develop future cyber talent.

Cyber Security for the Wider Good
Actively sharing intelligence and knowledge to build a more resilient and prosperous digital economy.

Committed to Sustainable Business
A carbon negative business, focused on reducing our footprint across all aspects of our growing team.

Broad Capabilities Built On Expertise

24/7 MDR & Security Operations Centre
No matter what time or day we are trusted to protect the UK's most critical national infrastructure.

Strategic Insight and Technical Expertise
Born from consulting, combining transformative security with technical skills to detect and protect.

Continuous Training and Development
Investing heavily in keeping our passionate team's skills updated, helps them and your business thrive.

Bridewell

Cyber Security. Where it Matters.

bridewell.com
+44 (0)3303 110 940
hello@bridewell.com