Navigator

Industrial Cybersecurity Consulting & Managed Services 2025

1898 & Co.

navigator.westlandsadvisory.com

Introduction

Operational Technology (OT) environments are foundational to critical infrastructure and industrial operations. These systems control physical processes essential to energy, transport, manufacturing, and public services. As connectivity increases, so does exposure to cyber, physical, and operational risks. Yet, despite the criticality of these processes, cyber maturity remains relatively low, with significant obstacles to accelerating improvements in cyber resilience.

Growing investment in digitalisation and tightening regulation - combined with complex operations and distributed assets and resources - all contribute to the challenge faced by Risk Leaders.

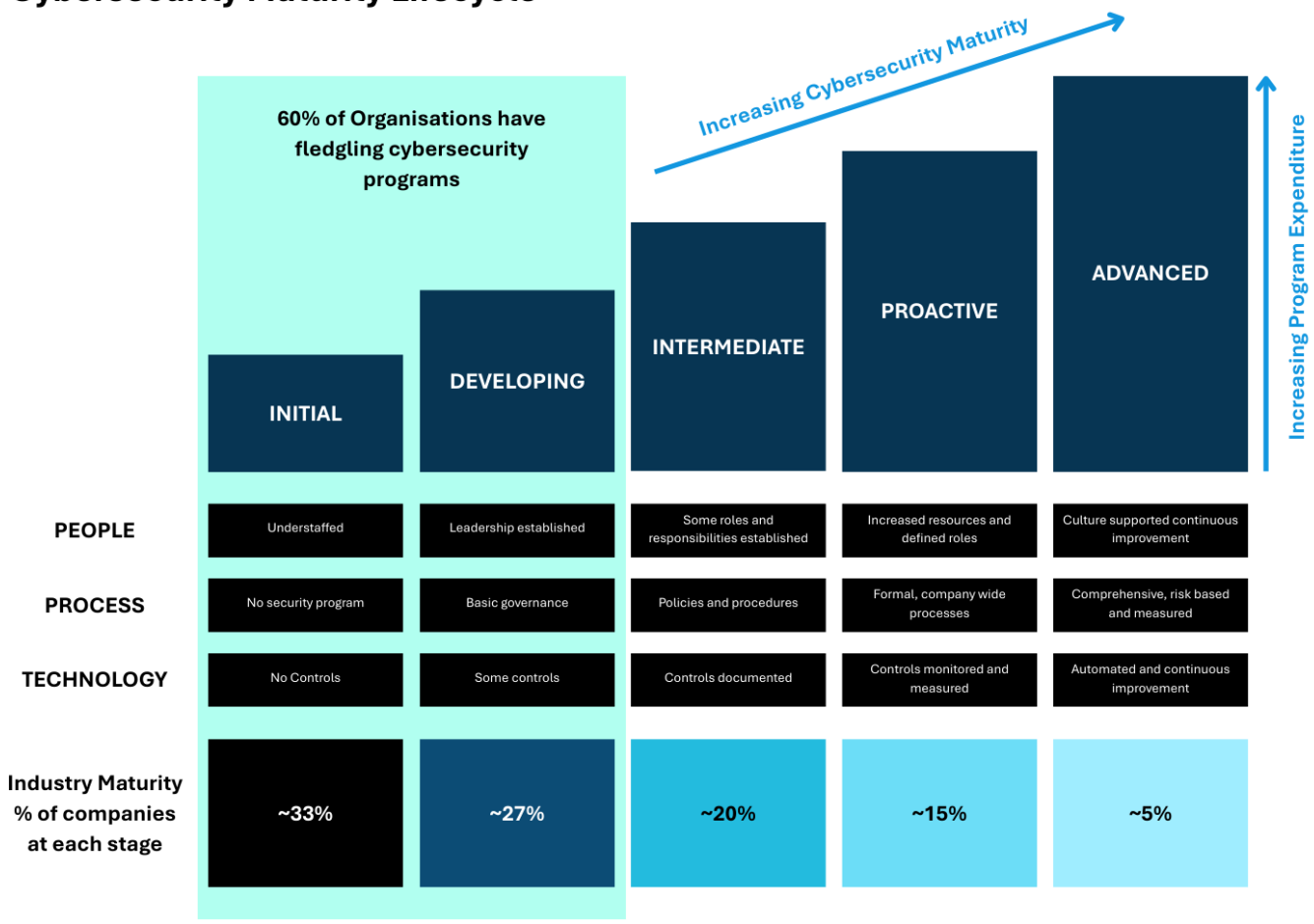
Change takes time and requires the alignment of people, processes, and technology. As a result, asset owners increasingly need the expertise that security consulting and managed services organisations can offer, bringing the technical knowledge, understanding of operational risk, and transformation skills needed to help move towards a more resilient operating model. This has resulted in a significant increase in expenditure on OT cybersecurity services with Westlands Advisory's (WA) latest market forecast projecting average growth of 18% per year to 2031.

Security consulting companies come in different shapes and sizes, and their effectiveness can vary widely depending on the requirement. Depth of knowledge and service quality often differ significantly by industry, region, and capability area. Understanding this variation - and matching the right service partner to the right context - is essential for Risk Leaders seeking to improve OT resilience.

Market Context

Many asset owners are still at the early stages of the cybersecurity lifecycle. WA estimates that 60% of organisations have no or fledging security programs with basic governance and controls. Many of these organisations are small to medium sized business with no regulatory drivers. Moving along the maturity pathway industries organisations tend to be international with stronger regulatory requirements related to cybersecurity and operational safety.

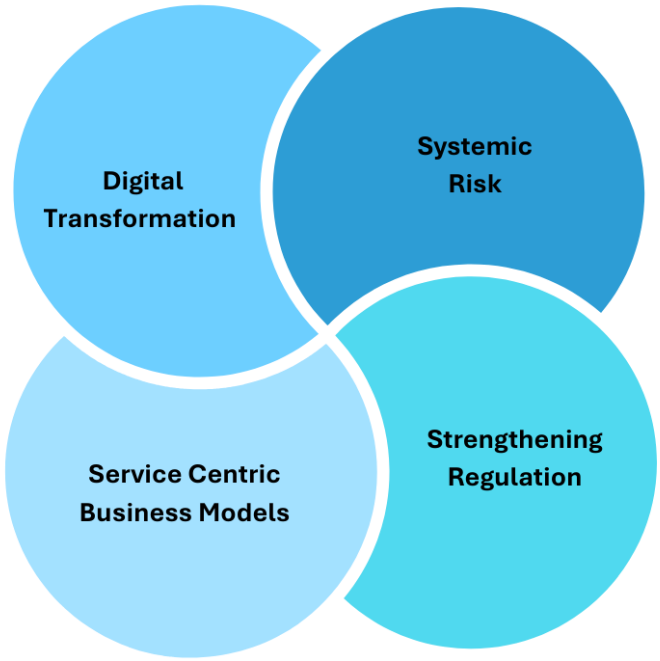
Cybersecurity Maturity Lifecycle



The three main market forces - digitalisation, risk, and regulation - continue to shape how asset owners approach cybersecurity and what they need from service partners. In addition to these forces, Westlands Advisory has added a 4th driver of investment which is the increasing service-centric transformation of OT cybersecurity, the shift from buying cybersecurity products or point-in-time projects to consuming ongoing, integrated cybersecurity capabilities as services. In the OT context, it means that asset owners are increasingly turning to external partners to deliver, manage, and maintain security outcomes.

Investment in OT cybersecurity has been consistently strong over the last 5 years, with investment doubling between 2020 and 2024. This reflects the relatively low level of cybersecurity maturity with organisations investing in tools to discover assets and manage vulnerabilities. However, the market has moved considerably. Whilst cataloguing assets, vulnerability management and threat detection remain imperatives, leading OT Risk Leaders have moved beyond these processes to build scalable and resilient operations aligned to business objectives. This growing maturity has been driven by the four market forces.

Market Forces Driving OT Cybersecurity Investment



1. Digital Transformation

OT environments are undergoing a significant shift. Once air-gapped and standalone, they now sit at the centre of complex, connected digital ecosystems. The adoption of cloud, remote operations, and edge computing is transforming how organisations design, run, and optimise industrial operations.

In this environment, traditional perimeters no longer apply. Instead, resilience depends on being able to enforce trust at the point of interaction: identity-based access, real-time monitoring, and strict segmentation across both north-south (IT to OT) and east-west (within OT) traffic flows.

Service providers must be capable of securing distributed environments at scale. This includes architecture for edge visibility, governance for connected assets, and controls that extend to endpoints, 5G infrastructure, and vendor-access portals.

2. Systemic Risk

Industrial operations face multiple risks to their availability and safety, stemming from both intentional and unintentional actions. While sophisticated nation-state attacks are relatively rare, the more common threat comes from criminal networks targeting IT systems or IT-connected assets within OT environments, often through ransomware. In addition, supply chain compromises and physical attacks also pose significant risks.

OT cybersecurity services must go beyond network security or device hardening. They must support multi-layer threat modelling, coordinated response between digital and physical domains, and rapid containment strategies that prioritise operational continuity and safety.

3. Strengthening Regulation

As critical infrastructure has become a focus of national security, governments and regulators have strengthened existing regulations and introduced new ones, shifting from broad guidance to specific, enforceable obligations.

In the US TSA directions demand formal incident response planning, detection capabilities, and board-level accountability for transport operators, whilst CIRCIA mandates that critical infrastructure reports significant incidents to CISA within 72 hours.

In Europe, NIS2 expands the scope of early regulation, sets maturity baselines, and introduces penalties for non-compliance across a wide range of industry segments. The EU Cyber Resilience Act (CRA) places new requirements on manufacturers and software providers to embed security into design and lifecycle management. The UK's Cyber Security & Resilience Bill is expected to pass through Parliament in 2025, expanding the scope and regulatory powers of its predecessor.

In the Middle East, Saudi Arabia and UAE have introduced local regulation related to critical national infrastructure protection and data sovereignty, whilst across Asia countries continue to strengthen policy, regulation and align to international standards (e.g. Australia, Japan, and Singapore).

Compliance is no longer separate from security. It must be embedded into service delivery with providers offering risk documentation, playbooks, reporting support, and roadmap planning tied to regulatory timelines.

4. Service Centric Business Models

One of the most significant shifts in the OT cybersecurity market is the growth of service-centric business models. Rather than purchasing standalone tools or commissioning periodic consulting engagements, asset owners are increasingly consuming cybersecurity as an ongoing service that is structured, measurable, and aligned to resilience outcomes.

In practice, this means organisations are not just outsourcing tasks like vulnerability scanning or remote access management but are engaging providers to deliver end-to-end capabilities, including maintaining response readiness, managing third-party access across industrial estates, embedding security into engineering projects, and correlating

threats across IT and OT. These services are increasingly delivered with defined service-levels and measurable outputs.

This model is being accelerated by the evolution of underlying tools and platforms. Cloud-based landing zones offer pre-integrated, policy-compliant environments that reduce deployment time and complexity across distributed OT estates. Generative AI and automation are helping providers scale expertise, supporting faster incident analysis, alert summarisation, policy creation, and executive reporting. Orchestration platforms are making it easier to consolidate fragmented telemetry into meaningful, actionable workflows.

These forces — digital transformation, risk, regulation, and security services — have changed the OT security mandate. Organisations can no longer rely on perimeter thinking or reactive practices. Leading asset owners are focussed on resilience by design, supported by capabilities that span detection, protection, governance, and recovery.

Aiming for Business Resilience

As industrial systems become more connected, more complex, and more critical to business continuity, the concept of resilience has become central to cybersecurity strategy.

Resilience in this context is not about preventing every incident. It is about being able to anticipate, absorb, and recover from disruption without losing control of operations, compromising safety, or undermining customer and stakeholder trust.

The World Economic Forum's Unpacking Cyber Resilience report (November 2024) frames this well:

"Cyber resilience is an organization's ability to minimize the impact of significant cyber incidents on its primary goals and objectives."

For OT environments, these goals are uniquely operational. The priority is not just protecting data or devices, but maintaining safe, stable, and available physical processes whether that is running a turbine, managing a power grid, or keeping a production line online. Whilst traditional cybersecurity programs often focus on preventing incidents and meeting compliance requirements, resilience asks more strategic questions.

- Can we detect disruption early enough to take action?
- Can we contain an incident before it becomes a systemic failure?

- Can we recover operations quickly, safely, and in a coordinated way?

In this sense, resilience is not just a technical goal but a business capability. It requires risk-aligned governance, cross-functional ownership, contingency planning, and operational ability to respond under pressure.

It also recognises that threats do not respect organisational boundaries. A cyber incident in IT can cascade into OT. A compromise at a supplier or contractor can create ripple effects across the supply chain. A power outage, network failure, or system misconfiguration can be just as disruptive as a malware infection.

Resilience reframes cybersecurity as a continuous business risk management process that is comprised of five core capabilities. Leading OT Security Service firms should be able to help asset owners address all of these.

Achieving Cybersecurity Resilience

1. Visibility and prioritisation: Clear understanding of assets, dependencies, and risks — especially for the most critical systems.

2. Layered protection: Segmentation, remote access controls, endpoint hardening, and perimeter enforcement to limit exposure and contain spread.

3. Integrated governance and decision-making: Defined roles, shared policies, and cross-functional coordination and collaboration between engineering, security,

operations, and executive leadership.

4. Managed Security Operations: SOC delivery models based on ongoing monitoring, management, and threat containment with a focus on maintaining safe and continuous operations.

5. Incident response and recovery readiness: Playbooks, tested procedures, offline backups, and clear escalation pathways that reflect the realities of industrial operations.

6. Sustained maturity through lifecycle integration: Security embedded into procurement, engineering design, transformation initiatives, and ongoing risk management.

These elements are not delivered by technology alone. They require expertise, operational awareness, and cultural change. This is why OT cybersecurity services are becoming an essential part of how organisations deliver resilience at scale.

OT Resilience Challenges Faced by Asset Owners

While the case for improving OT cybersecurity is increasingly well understood, execution remains difficult. Asset owners face persistent challenges that the right services can help overcome. This includes helping asset owners to understand the challenge, communicate the problem, deliver the business case, pilot the solution, deliver the program, and manage the security operation. Security consulting organisations have evolved to provide expert support throughout the security lifecycle, addressing ten key challenges .

1. Measuring Resilience and Proving Value: Many organisations still struggle to define what good OT cybersecurity looks like. Resilience is often treated as an aspiration, not a measurable objective. Metrics for uptime, recovery readiness, and risk reduction are not always in place making it difficult to set priorities or secure long-term investment. Many asset owners struggle to move beyond compliance checklists to performance-based metrics. Questions like “Are we resilient to ransomware?” or “How long would recovery take?” remain hard to answer. This makes it difficult to set priorities, build confidence, or justify budget.

2. Business Case and Return on Investment: Unlike traditional IT programs, OT cybersecurity investments are often preventative, with no immediate cost savings or productivity gains. This can make it difficult to secure funding. Business leaders may struggle to understand the risk-reduction benefits or to justify spend against other

operational priorities. Linking cyber investments to resilience outcomes — such as downtime prevention or regulatory assurance — is critical but not always well articulated.

3. Ownership & Organisational Alignment: OT cybersecurity cuts across multiple departments from engineering and operations to IT, procurement, legal, and executive leadership. Without clear ownership and structured collaboration, initiatives stall or become fragmented. Internal misalignment on roles, funding, and priorities often creates confusion and inaction.

4. Legacy Environments: Many OT systems were never designed with cybersecurity in mind. Equipment may run on outdated operating systems, lack patching capability, or use proprietary protocols with no visibility. Even understanding what is in the environment can be a significant task.

5. Governance & Regulatory Compliance: Compliance obligations are increasing across sectors and jurisdictions, from NIS2 to NERC CIP and TSA directives. For many organisations, staying ahead of shifting regulatory demands while maintaining operational performance is a significant burden. Governance models must evolve to integrate cybersecurity into broader enterprise risk and control frameworks.

6. Talent Shortages and Skill Mismatches: There is a shortage of professionals with both cybersecurity expertise and operational experience. Asset owners often rely on small internal teams who cannot keep pace with the growing scope of threats, regulatory requirements, and technical complexity.

7. Fragmented Tools and Telemetry: Most OT environments accumulate a patchwork of tools over time — firewalls from one vendor, anomaly detection from another, with separate asset inventories and alerting platforms. This is multiplied in complex, heterogenous sites where multiple control systems using different security tools and policies exist. Without integration, the result is noise, duplication, and blind spots. The complexity of managing these tools undermines visibility and incident response.

8. Balancing Security with Operational Needs: Operations teams are rightly focused on uptime and safety. Changes that introduce latency, risk downtime, or interfere with automation are often resisted. Security initiatives must be tailored to fit operational requirements. This can delay or dilute security measures unless cross-functional governance is in place.

9. Aligning with Business Priorities and Digital Transformation: Many asset owners are accelerating digital transformation and connectivity between IT and OT systems. This brings opportunities for efficiency, data-driven optimisation, and remote operations but it also introduces significant security and scalability concerns. As more enterprise

applications and analytics platforms connect to OT data sources, organisations must manage increasing IT connectivity within traditionally isolated environments.

Security teams must work closely with business units and engineering teams to align priorities, avoid disrupting core processes, and ensure that cybersecurity does not become a barrier to innovation. This requires scalable architectures, consistent governance, and services that balance control with operational agility.

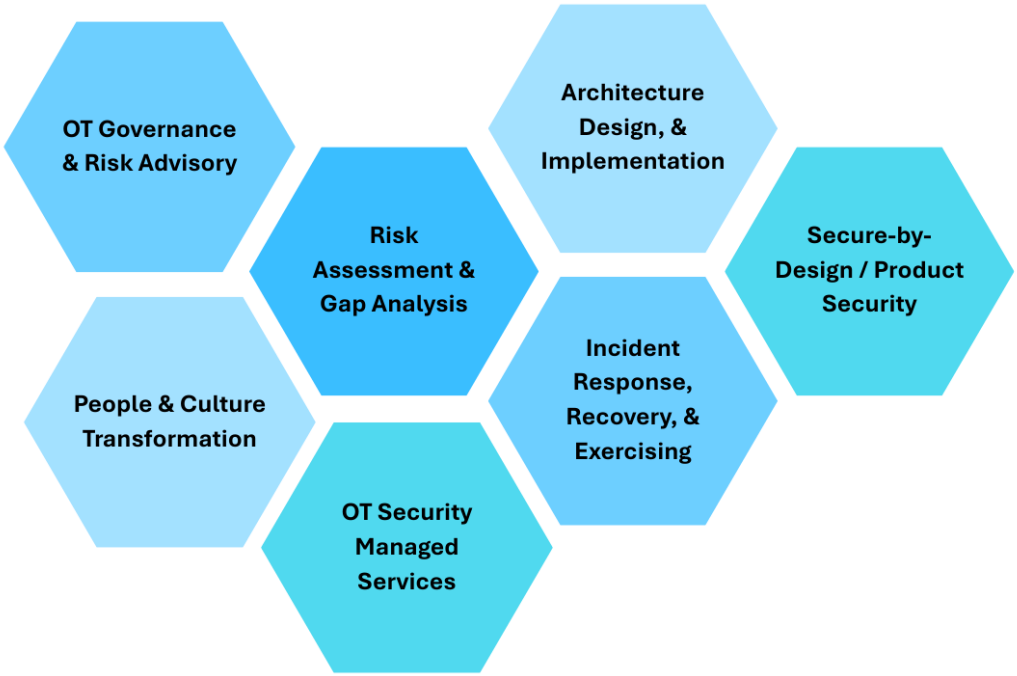
10. Managing Remote Access and Third-Party Risk: Industrial systems often rely on external vendors and OEMs for maintenance. Remote access solutions are essential but also bring risk. Without strong control over who has access, when, and how, organisations expose themselves to unmanaged entry points and monitoring blind spots.

Many of these challenges are not new but they are intensifying as connectivity and cyber risk grow. They explain why many asset owners turn to external services: not just for technology, but for strategy, implementation, and resilience. Effective services must be context-aware, flexible, and delivered by teams who understand industrial realities.

OT Cybersecurity Services

Delivering resilience in OT environments requires a range of specialised services that align with how industrial systems are built, maintained, and operated. These services extend far beyond compliance or intrusion detection, helping asset owners implement layered protection, reduce exposure, prepare for incidents, and continuously adapt to change. Services are sequential, helping organisations to build the governance model, assess risk and then implement the technology and processes to improve resilience. Leading firms also guide partners of product security, ensuring security is built into products and systems prior to commissioning. Managed Security Services and Incident Response provide ongoing operational support to asset owners.

OT Cybersecurity Professional Services



1. OT Governance and Risk Advisory

Governance is the foundation for any OT security program. It provides clarity on roles, responsibilities, and acceptable risk levels. In OT, effective governance means more than adopting IT frameworks, it requires adapting risk models to account for physical processes, legacy systems, and safety constraints. Strong governance prevents ambiguity in a crisis and builds the foundation for secure decision-making. It becomes especially critical in multinational operations, where different sites face different regulatory expectations. Services that help harmonise governance across countries and regimes are increasingly valuable.

Services typically include development of OT-specific security policies, creation of cross-functional governance models spanning IT, OT, physical security, and compliance, and regulatory mapping.

2. Risk Assessment and Gap Analysis

Before anything can be secured, it must be understood. OT environments often contain undocumented assets, outdated systems, and hidden interdependencies. Risk assessments are the diagnostic service, providing visibility into these realities and helping organisations prioritise investment. They should build an asset inventory, uncover where protective controls are missing and where recovery time objectives are unrealistic,

enabling asset owners to prioritise activities and invest in the appropriate people, processes, and technology.

Key service elements include both passive and active asset discovery, vulnerability assessments tailored to OT system constraints, and threat modelling and risk quantification.

3. Architecture, Design, and Implementation

Well-structured OT networks are the first line of protection. Architecture services support the design and implementation of security controls that reduce exposure and limit the spread of threats. Architecture and design services do not just reduce the risk of a breach, they reduce the likelihood that an incident becomes a crisis. Effective segmentation and remote access controls are among the most impactful, yet under-implemented, protective measures in industrial environments.

Core considerations include:

- Network segmentation: Both north-south (IT/OT separation) and east-west (between zones of the OT environment). This minimises lateral movement and isolates critical functions.
- Perimeter defences: Firewalls, demilitarised zones (DMZs), and intrusion prevention tuned to industrial protocols.
- Remote access security: Time-bounded access, MFA, jump servers, session logging, and least privilege access — especially important for OEMs and integrators.
- 5G integration: For operations using private 5G networks or edge-connected devices, architecture must address SIM provisioning, MEC security, and identity-based access at scale.

4. Secure-by-Design / Product Security

Secure-by-design integrates protection into the entire lifecycle of OT systems from engineering concept to commissioning, ensuring that new assets do not introduce new vulnerabilities. It also includes product security, a fast-growing consulting segment focused on the design, testing and lifecycle management of internet connected products. This in part is being driven by the EU's Cyber Resilience Act that, although focussed on Europe, requires all imported products to be secure-by-design and with software support provided throughout its lifecycle. Services include design reviews and security validations and hardening procedures for controllers, sensors, and HMIs.

5. People Consulting & Workplace Transformation

People and workplace transformation services focus on building shared understanding, clear roles, and operational readiness across all levels of the organisation. This goes beyond basic awareness training to cultural transformation and change management. Services range from executive and board education, to upskilling OT engineers, integrated awareness campaigns, scenario-based testing and training, and stakeholder alignment.

These services help organisations build a culture of accountability. They enable fast response in a crisis, reduce miscommunication between IT and OT, and ensure that security is viewed as a shared responsibility.

6. OT Security Management Services

Ongoing security operations in OT differ from IT. These services manage controls, detect anomalies, and support remediation — all with industrial constraints in mind. These services also help rationalise alert noise, integrate fragmented tools, and bridge gaps between IT and OT telemetry. As environments grow more complex, the ability to consolidate and contextualise data will become essential.

7. Incident Response, Recovery, and Exercising

Effective incident response in OT must account for physical processes, safety systems, and interdependent assets. These services prepare organisations to respond, contain, and recover. Services include playbook development and OT-specific runbooks and digital forensics with industrial context. It also includes backup and recovery strategies for OT assets.

Exercising is important for testing readiness and continuous improvement. These services help organisations learn from past incidents, stress-test assumptions and can reveal flaws in governance, tooling, and assumptions. Key activities include tabletop and live-fire exercises, lessons-learned programs following real-world events, and scenario modelling for future-state risks.

Evaluating and Selecting OT Cybersecurity Partners

Selecting the right cybersecurity partner is not a one-size-fits-all decision. Asset owners have unique needs based on their size, operation, regulatory exposure, maturity level, and internal capacity. Evaluating partners effectively means understanding what kind of

support is needed and what capabilities a provider must bring to deliver meaningful results.

Different Buyers, Different Needs

The most successful relationships are based on a clear understanding of context. Buyers should assess not just who can do the work, but who can do it in their environment. A well-matched partner accelerates maturity. A mismatch drains time, budget, and credibility. Storytelling, case studies, and scenario-based proposals can help both sides understand how the partnership will work in real conditions. This is where many relationships start, testing concepts in OT Lab environments to help align around needs and requirements.

For organisations at the start of the cybersecurity maturity process, the focus should be on visibility, basic segmentation, governance setup, and secure remote access. Partners must bring empathy, explain complexity, and avoid overengineering. For those that have run pilot projects and are advancing the program, help is required to integrate tools, formalising response capabilities, and operationalising risk frameworks. Finally, those that require support scaling across business units, benchmarking controls, enhancing recovery readiness, and embedding security-by-design in every new investment will require partners with specialist skills. Depending on size, scale and maturity of the asset owner, different services are required.

Multinational Operators face complexity at scale. They often must coordinate across sites, jurisdictions, and business units, each with different infrastructure and risk profiles. A global energy company, for instance, may need a partner who can harmonise governance across EU and U.S. regulations while delivering localised SOC services in multiple languages. Projects often start as pilots before scaling across global sites. Key needs include cross-border regulatory alignment, scalable monitoring, integration with global IT and engineering teams and preferred partners include mature MSSPs, global integrators with strong OT capabilities, and regional specialists who can support local delivery.

Sovereign or State-Regulated Entities such as national grid operators, water utilities, or public transport providers often prioritise local compliance, trust, and assurance. They may face political or public accountability that global players do not. Key requirements include national data residency, sovereign service delivery and audit readiness. Preferred partners are generally trusted national providers, organisations active in public-sector resilience programs, or government-certified vendors.

Mid-Sized Manufacturers or Industrial Operators may be earlier in their cyber maturity journey. Often lacking internal teams or budgets to run complex programs, they benefit most from partners who can offer pragmatic, stepwise support. This includes risk assessment, prioritised roadmap, foundational governance, and turnkey services and is

generally serviced by niche OT security firms and regional MSSPs with experience in brownfield environments.

Different Service Providers, Different Strengths

Just as OT asset owners vary in maturity, industry, and complexity, so too do the service providers that support them. The OT cybersecurity market is not homogenous — it draws on a diverse ecosystem of players, each shaped by their heritage, core competencies, and go-to-market models.

Understanding what type of partner to engage with and where they excel helps Risk Leaders set realistic expectations and assemble complementary capabilities when needed.

Few service providers can meet every OT cybersecurity need. Asset owners must look beyond branding and assess how a supplier's strengths align with their own maturity, risk profile, and operating model. Sometimes the right answer is a mix of service partners — with roles clearly defined and managed under a cohesive strategy.

- **Global Professional Services Firms** bring depth in governance, regulatory alignment, program design, and cross-sector benchmarking. They often lead major transformation programs and help build board-level engagement. Strengths include strategic advisory and transformation roadmaps, multi-national compliance and enterprise integration, and CISO-level engagement and stakeholder alignment. In addition to traditional advisory services, leaders have built teams with deep OT technical expertise and engineering experience, developed OT specific playbooks, and introduced technology to accelerate and scale OT cybersecurity deployments. They have the infrastructure, people, and processes to lead complex end-to-end engagements.
- **Original Equipment Manufacturers** have deep technical knowledge of the systems they provide and are increasingly investing in embedded cybersecurity capabilities and services. Strengths include engineering-level knowledge of specific control systems and strong lifecycle support. Two camps have emerged. One group who has acquired and built technology solutions and provide vendor agnostic services (e.g. Honeywell, Rockwell Automation, Siemens), and the second group who exclusively services its own systems (e.g. Emerson Electric and ABB).
- **Global IT Services and Infrastructure Providers.** These firms offer strong capabilities in managed services, cloud integration, and SOC operations, often extending existing enterprise IT relationships into the OT domain. Strengths include SOC/SIEM maturity and platform integration, Identity and Access Management capabilities and large-scale managed detection and response offerings.
- **Engineering Services Firms and Systems Integrators.** Rooted in plant design, control systems engineering, and infrastructure buildout, these firms are increasingly building

cybersecurity into their industrial project offerings. Strengths include process control and automation experience, ability to integrate security into capital projects, and trusted relationships with plant and maintenance teams.

- **Cybersecurity Services Specialists.** Pure-play security firms focus exclusively on cybersecurity. Some specialise in OT/ICS environments, bringing field-experienced professionals, advanced threat modelling, niche forensics, and rapid incident response. Others have a significant IT consulting and managed service background with a strategic focus on growing OT capabilities and capacity. These providers often offer deep technical insight and may work alongside larger contractors. They are best suited for country/regional specific knowledge, high-assurance environments, regulated sectors, or organisations looking for specialist capabilities.
- **Mobile Network Operators** bring large-scale MSSP capabilities and deep insight into network-level threats — including lateral movement, remote access abuse, and edge vulnerabilities. Their value proposition lies in stopping threats at the network level before they reach OT systems, leveraging strong visibility, analytics, and response infrastructure. Asset owners prioritising secure remote access, 5G-enabled operations, or who require strong perimeter defence integrated with telco infrastructure may consider working with MNOs who can also demonstrate strong understanding of OT networks.

Evaluating partners

Asset owners often work with a range of partners. This may be driven by OEM agreements, preferred supplier contracts, or a need for specialist skills. The ideal partner understands that OT cybersecurity is not about selling software but is about building trust, adapting to industrial realities, and helping the organisation build durable capabilities. Buyers should look for partners who can demonstrate outcomes, not just offer services. Long-term resilience comes from relationships rooted in shared understanding and ongoing support.

There are however some key considerations that asset owners should consider based on their specific requirement.

1. Service Capability and Lifecycle Coverage

Can the provider support the full OT cybersecurity lifecycle — from assessment and architecture to managed operations, response, and recovery? Do they offer tailored pathways for organisations at different maturity levels, and do they have the necessary accreditations?

2. OT Experience and Field Expertise

Security strategies that ignore the realities of the plant floor often fail in implementation. From interviews with CISOs and engineering leaders it is clear that security consulting firms with strong OT credibility build trust amongst the engineering teams and accelerate program delivery. Does the team include professionals with real-world OT experience — plant-side engineers, ICS specialists, safety managers? Certifications like IEC 62443 or GICSP are good signals, but experience is equally important.

3. Tools, IP, and Resources

Repeatable delivery, innovation, and efficiency come from having structured, proven resources. This includes OT labs and testing environments, cloud landing zones, unique tools (e.g. GenAI for governance or risk scoring), and proprietary processes, frameworks, or benchmarking methods.

4. Integration and Technology Flexibility

Can the provider integrate with legacy systems, cloud telemetry, and diverse industrial protocols? Are they vendor-agnostic? Can they consolidate alerts across environments to deliver meaningful context?

5. Ecosystem and Partner Collaboration

Do they have relevant partnerships — with OEMs, cybersecurity vendors, cloud providers, and national CERTs or ISACs? Can they coordinate effectively across a complex vendor landscape?

6. Geographic Reach and Regulatory Responsiveness

Multinational operators need global capability — but local fluency. And regulated entities need partners aligned with state and sector expectations. Can they provide localised support, data residency assurance, and respond to national requirements across multiple jurisdictions? Are they active in regulated or sovereign sectors?

7. Sector-Specific Knowledge and Understanding of Operational Risk

Sector familiarity leads to faster risk prioritisation, better playbooks, and stronger response. Have they worked in the relevant sector? Do they understand its business drivers, operating models, and unique threats? Are they active in relevant knowledge-sharing communities?

Concluding

Digital convergence, systemic risk, and strengthening regulation necessitates that OT cybersecurity evolves beyond technical protection toward true operational resilience. Asset owners face a future where cyber threats, physical disruptions, and business pressures are inseparable and where resilience is the foundation for value protection, service continuity, and trust.

The security services landscape is growing in sophistication, but challenges remain. Asset owners must seek consulting partners who understand operational realities, who can integrate cybersecurity into enterprise risk governance, and who can continuously adapt security capabilities as technologies, risks, and regulations evolve.

The future demands more than detection and compliance. It requires services that:

- Align cybersecurity directly with business value and operational risk.
- Integrate cyber, physical, and operational resilience into a unified model.
- Enable dynamic adaptation, not just static protection.
- Build governance frameworks that scale across jurisdictions, suppliers, and sites.
- Augment human decision-making with AI and automation, accelerating recovery as much as detection.

Resilience should be viewed as an organisational capability, not a standalone product or project. It requires leadership, a unified vision, and continuous evolution and testing and a trusted consulting partner with deep expertise in OT, cybersecurity and delivering complex solutions.

Profile: 1898 & Co.

Introduction

1898 & Co. has been recognised as an Innovator in Westlands Advisory's Industrial Cybersecurity Consulting and Managed Services Navigator 2025. 1898 & Co. is a global business, technology, and security consultancy serving critical infrastructure industries. The organisation supports asset intensive industries with asset planning, business transformation and cybersecurity via its 24×7×365 Advanced Threat and Protection Centers in Houston, Texas, and Mumbai, India.

The cybersecurity business includes Facility Cybersecurity (the protection of large complex sites), Security Consulting Services (IT and OT systems) and Managed Security Services. As part of Burns & McDonnell, with 120 years of industry experience, 1898 & Co. understands the complexity of asset-intensive business models and the trends impacting these industries. The organisation has focussed strongly on working with brownfield customers to accelerate cyber resilience, and its operations also cover greenfield installations and new verticals.

Positioning & Strategy

Burns & McDonnell and 1898 & Co. employ professional staff across more than 70 global offices, helping customers improve processes and streamline operations—including cybersecurity. The organisation had the foresight to recognise an emerging requirement among asset owners for specialised services to accelerate and scale OT cybersecurity operations, driven by increasing digital transformation and tightening regulations. This led to the formation of cybersecurity and managed security services through 1898 & Co., which has since emerged as one of a select group of cybersecurity service firms dedicated to providing resilient industrial operations.

1898 & Co. draws on a talent base offering deep understanding of industrial systems, cybersecurity, and business transformation. Its cybersecurity team has extensive OT sector experience, with strong knowledge of regulatory frameworks such as TSA, NERC-CIP, IEC 62443, and NIST, as well as industrial automation, control systems, and security operations.

The company supports customers across the full cybersecurity lifecycle, from security design through to operational management. Its consulting and design services are complemented by a rapidly growing managed security services business, which meets

the increasing demand from asset owners' management of OT cybersecurity tools and operations.

1898 & Co. has strong partnerships with all major industrial cybersecurity (IDS) vendors, along with several niche providers of risk and threat intelligence services. It also leverages its own platform to deliver managed security service.

While most of its customer base is in North America, 1898 & Co. has the infrastructure and experience to support globally distributed operations and is actively expanding its international footprint to provide scalable, global service delivery. Key sectors served include power, oil, gas and chemicals, manufacturing, pipelines, aviation, water and wastewater, and government. Manufacturing is a rapidly growing vertical. Customer retention rate across industries exceeds 90%, underscoring high levels of satisfaction and trust in their services.

Capabilities

1898 & Co. provides a broad suite of services tailored to the needs of industrial and critical infrastructure operators:

OT Governance & Risk Services are built on deep knowledge of compliance and regulatory requirements (including NERC-CIP, IEC 62443, and the DoD Risk Management Framework), 1898 & Co. helps organisations develop detailed governance strategies and implementation plans. Risk Assessment services cover both cyber and physical vulnerabilities through on-site assessments, attack simulations, and penetration testing. The emphasis is on understanding operational context to accurately assess business risk.

Architecture, Design & Implementation is a key strength. The company applies a consequence-driven, cyber-informed engineering approach. Whether integrated into customer teams or working alongside Burns & McDonnell, 1898 & Co. architects, designs, and implements cyber/physical controls. Its facility cyber design services incorporate cybersecurity into new builds and processes from the ground up, covering design, commissioning, and accreditation.

1898 & Co. has significant experience in People Consulting & Workplace Transformation. Delivered by experienced strategy and functional consultants, this includes workforce training, tabletop exercises, and broader advisory services to help embed security culture and capability.

Managed Security Services are delivered from two 24/7 Advanced Threat and Protection Centers (SOCs) in the U.S. and India. While the platform is optimised for OT networks, it is also deployed across enterprise (IT and OT) environments. Incident Response, Recovery & Training is supported by cross-functional teams working across the entire client cybersecurity journey—from initial network design to incident response. Services include

industrial incident response planning, hands-on training for in-house staff, proactive threat hunting, and both on-site and remote response support during OT or IT incidents.

Market Perception

1898 & Co. is recognised for a deep level of experience in the field and has a growing reputation as a strong partner through continued investment and innovation in its platform and services. Notable differentiators include the organisations strong understanding of plant design and processes, cross functional teams and managed security services, and asset management.

Deep Insight into Security Design and Processes: Strong relationships with OEMs and security platform vendors enable 1898 & Co. to offer extensive insights into managing the security posture and responding to incidents across assets and devices. This foundation enables 1898 & Co. to deliver a customized approach, while assessing and managing security posture and incident response. Cyber operations are further strengthened by a comprehensive, custom-built library of OT/ICS/BMS security policies.

Cross Functional Energy and Transportation Experience: The company has a significant portfolio of project experience working with the utility and energy transportation sectors, including over 550 power utilities. Other prominent sectors served include oil, gas and chemical companies, manufacturing, ports and maritime, and transport electrification. Cross Functional teams advise on acquisition & divestment; asset planning & management; business strategy & transformation; technology including data & analytics; financial analysis; and policy & regulation. Burns & McDonnell design & build industry rankings (ENR) include #1 in power, #1 in pipeline, #4 chemical plant, #5 Food & Beverage, #6 Pharmaceutical, #12 in wastewater treatment and #14 in manufacturing design.

Asset Management Experience: Asset visibility and management is a perennial challenge for infrastructure operators and 1898 & Co. is well positioned to support its customers. The company has a deep knowledge of industrial assets and a portfolio of services to help customers plan and manage assets at a sector level (e.g., energy transmission & distribution, food & beverage).

Industrial Cybersecurity Consulting and Managed Services 2025

The Industrial OT Cybersecurity Consulting and Managed Services Navigator is an evaluation of organisations with both significant experience and expertise of working with Asset Owners to improve OT cybersecurity resilience. Organisations are positioned as Leaders, Experts and Innovators. There is significant variation between organisations capabilities and ability to deliver, with organisations having different sector, regional, or

service strengths. Asset Owners should consider partners that are most aligned to their unique requirement.

Appendix

Definition

OT (Operational Technology) Cybersecurity Consulting and Managed Services refer to a set of expert-driven offerings designed to protect industrial systems and critical infrastructure from cyber threats and to ensure operational resilience.

This includes **OT Cybersecurity Consulting**, professional advisory services focused on identifying risks, improving security posture, and guiding the secure design, implementation, and governance of operational technology environments. This includes assessing the cybersecurity maturity of systems like SCADA, DCS, and PLCs; aligning with industry standards (e.g., IEC 62443, NIS2, NERC CIP); and developing strategies for

segmentation, secure remote access, asset visibility, and incident preparedness. This also includes ensuring OT governance maps to business requirements and IT operations, workplace transformation, and a growing focus on secure-by-design.

OT Cybersecurity Managed Services is the operational support provided by a third party to monitor, detect, and respond to cybersecurity threats targeting OT environments. These services often include 24/7 security operations (e.g., SOC), managed detection and response (MDR), patch and vulnerability management, secure remote access management, threat intelligence integration, and compliance monitoring, and incident response.

Evaluation

Service Vendors are assessed according to Competencies and Strategic Direction.

Competencies consists of the maturity of the services offered across (OT Governance & Risk, Risk Assessments, Architecture Design & Implementation, Secure-by-Design/ Product Security Advisory Services, People Consulting & Workplace Transformation, OT Security Managed Services, and Incident Response, Recovery & Training). This assessment totals 50% of the Competencies assessment. The remaining score is against 9 core competencies including People, Internal Operations, Security Operations, Technology, Market Reach, Execution, Partners, Customers and Business Performance.

Strategic Direction is an assessment of the company plans and strategy related to Vision, People, Investment, Internal Operations, Security Operations, Innovation, Market Reach, Partners, and Customers.

Methodology

The following information and insight contributes towards the Navigator research and conclusions. Westlands Advisory directly interviewed over 70 organisations - a mix of Service Vendors, Platform Vendors, CISOs, and Engineering Leaders.

- **Open Source**: Collection of all relevant open-source information on vendors including company documentation and information, reviews and 3rd party websites.
- **Questionnaire**: The Industry OT Cybersecurity Navigator 2025 vendor questionnaire is an important source of information. The survey is issued at the start of the process and is confidential, only being used for evaluating vendor performance.
- **Vendor Briefings**: Vendor briefings offer industry the opportunity to provide Westlands Advisory with insights into current capabilities, strengths and strategic direction. The purpose of the Vendor Briefing is to ensure that Westlands Advisory has the facts and

insight required to evaluate the companies' Capability Positioning and Strategic Direction.

- **CISO and Engineering Leaders**: Interviews with CISOs and Engineering Leaders to gain further insight into Service Vendor performance, strengths and weaknesses and views on the wider ecosystem.
- **Community Briefings**: Westlands Advisory gains insights from Platform Vendors and other channel partners into the relative strengths and weaknesses of different Service Vendors. Westlands Advisory also consults with industry experts on the market and services and has an independent consultation process to ensure that the process is fair and representative.

Qualification

Qualification for the Industrial OT Cybersecurity Services Navigator 2025 are outlined below.

- The organisation should have a minimum of 15 OT cybersecurity engagements in 2024 or revenues in excess of $10 million globally.
- The engagements are in at least 2 geographical regions and delivered by local teams.
- The organisation must have at least 1 OT cybersecurity SOC with OT security analysts.
- The organisation needs to demonstrate extensive knowledge and experience of working in OT environments.