WESTLANDS ADVISORY

Data. Insight. Strategy.

Industrial Security Consulting & Managed Services Navigator 2022

Synopsys

Westlands Advisory's 'Global OT Cybersecurity Industry Analysis' reported investment in OT cybersecurity services increased by 15%[i] in 2021. This is expected to continue over the next few years due to ongoing industrial digital transformation and the current low level of cybersecurity maturity. Whilst early adopters are optimising security programs, the majority of Industrial Operators are still at earlier stages of the cybersecurity lifecycle, characterised by low levels of digital asset awareness, inconsistent and poorly applied governance, and limited security controls. This is starting to change as organisations increasingly connect and digitalise operations, resulting in growing investment in services to assess risk, develop the security strategy, implement the controls, and manage the cybersecurity operation. Asset operators and risk leaders are faced with choosing a security partner from a growing number of service providers.

Digital Transformation of Operations

The digitalisation of industrial operations is advancing quickly. Whilst it is a truism that industrial operations are built to last 25 years and change is slow, it is also a fact that during the lifetime of a plant, sensors and controls are replaced to improve reliability and productivity. Digital products are creeping into brownfield manufacturing operations whilst newer sites are already connected and highly automated.

The pace of change is unlikely to slow over the next decade. Industry projections point towards annual growth of around 15% for industrial software and IIoT (Industrial Internet of Things) platforms. Yokogawa reports that 64% of industrial operators will reach the highest level of autonomy by 2030, up from 15% in 2023. Siemens predicts that 34% of organisations will have digital twins in productive use by 2023. A SANS[ii] Institute survey in 2021 highlighted the growing use of the cloud for OT applications, including remote monitoring of operations and access for third party managed services. Combining and synthesising all of the available research and opinion highlights a manufacturing journey towards self-optimising systems enabled by autonomy, 5G and cloud computing.

A key enabler of industrial transformation is cybersecurity. The era of the industrial system that is not connected to the internet has long since passed. This requires organisations to elevate cybersecurity from an afterthought to a strategic priority where security is a cornerstone of product development, manufacturing processes and supply chains.

Risk and Security Maturity

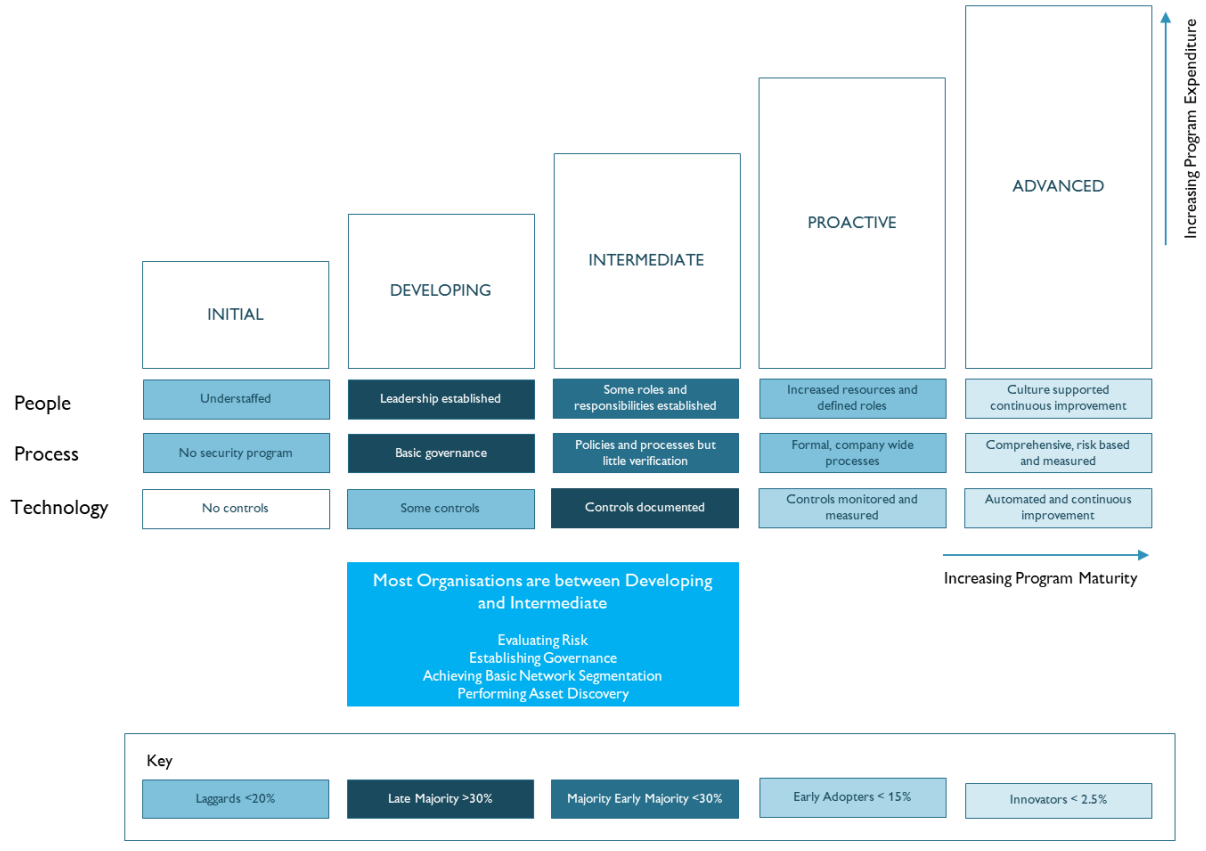
However, investment in digital programs can get ahead of security. In industrial markets, investment in the safety, reliability and availability of industrial systems has not always included security. There is a myriad of reasons why an organisation falls behind on its security program, from the often quoted "if it ain't broken, don't touch it" mentality, to the long-life cycle of industrial systems, and leadership disinclination to invest.

As noted in an earlier WA paper, "most asset owners are somewhere between the start of their security program and midway through updating and implementing basic security controls to achieve a strong and consistent baseline across their infrastructure." The previously mentioned SANS Institute paper provides an insight into current market maturity related to People, Process and Technology. According to the research, 24% of organisations have no formal process in place to detect threats in OT networks, whilst only 30% are using anomaly detection engines. By extension it's reasonable to assume that the majority have therefore not accurately mapped their assets. This is supported by a Ponemon Institute[iii] survey that reports only 29% of organisations have a complete inventory of IoT/OT devices.

There are signs that industrial operators are moving in the right direction. The SANS survey highlighted that security has risen to the second highest business concern in 2021 (46% of respondents from 39% two years earlier). Additionally, in 2019, 59% of organisations relied on internal resources for incident response, a high skilled process which many industrial operators are unlikely to be able to execute by themselves. By 2021 this had dropped to 44% as organisations increased investment in outside services.

WA's work supports these conclusions. Discussions with industrial operators, service providers, and technology vendors points to the majority of industrial organisations at the early stages of their security programs, somewhere between Developing and Intermediate. The typical industrial operator has not clearly outlined roles and trained staff, adopted a company wide cybersecurity policy, and is not proactively monitoring OT threats.

Industrial Cybersecurity Maturity Lifecycle



Growing choice of partners

Industrial Operators will require support as they increase program maturity yet finding the right partner amongst a diverse and expanding list of OT security service providers isn't necessarily straightforward. In many cases service providers have similar messages and capabilities. Before diving into discussions WA recommends that Industrial Operators create a short list of potential partners that are most aligned with the characteristics of their business. Is the requirement national or international, with a single site or multiple sites? Is the business driven by strict regulatory compliance? Is the need purely for OT network segmentation and threat detection, or is there a requirement to address security on the plant floor and across the manufacturing site? Is the requirement to implement basic security controls or is it part of a transformational manufacturing project?

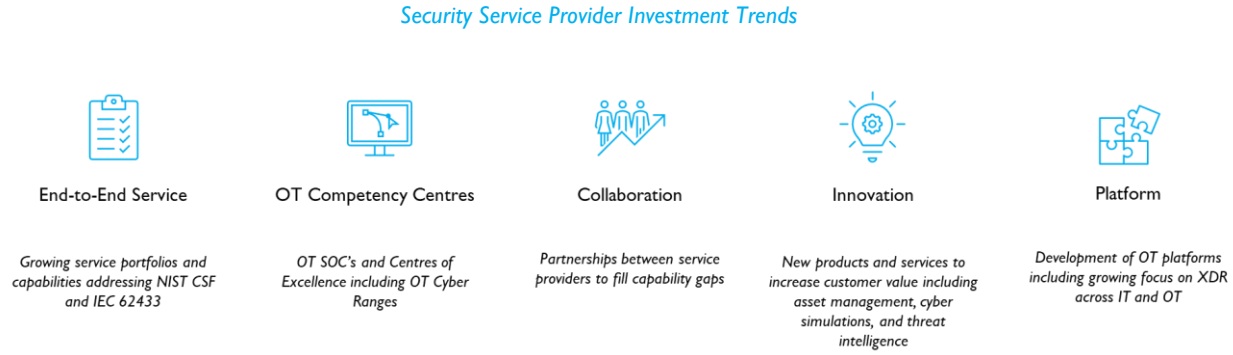
The answer to these questions will guide Industrial Operators towards a set of providers that will be more suited to addressing their challenge. For example, a regional utility operating in a highly regulated market with a clear requirement to understand its assets and to monitor OT network performance and threats, should consider an OT specialist with a local presence and strong knowledge of the vertical and related regulatory requirements. Conversely, an international Food & Beverage firm seeking to standardise its global cybersecurity strategy across its operations and supply chain is likely to require a partner that can manage large transformational projects, provide 24x7x365 monitoring globally whilst also offering localised support.

Industrial Operator Supplier Capability Considerations

The strengths and capabilities of different service providers are generally determined by the origin of company. These service providers tend to fit neatly into the following categories.

- *Professional Services Firms*: consulting expertise at scale, offering a full range of services globally
- *Engineering and Cyber*: industrial operating experience and strong OT security knowledge
- *Industrial Automation*: industrial control system expertise with an expanding range of cybersecurity services to address converging IT and OT operations
- *Telcos*: Industrial IT network monitoring and threat detection with growing OT security credentials
- *IT Services Firms*: combining strong IT security expertise with experience of designing, monitoring, and implementing industrial operations
- *Cybersecurity Services Firms*: security specialists with strong IT security capabilities that have evolved services to include OT

These companies provide customers with the end-to-end security services needed to help their partner deliver against IEC 62443, NIST CSF, CIS Controls or equivalents. Investment in people and capabilities is also growing amongst these firms, characterised by expanding services, OT competency centres and product innovation.



Industrial operators looking for a partner that can help them move from the "Developing" stage to an "Advanced" security program should consider organisations that are able to provide a range of services.

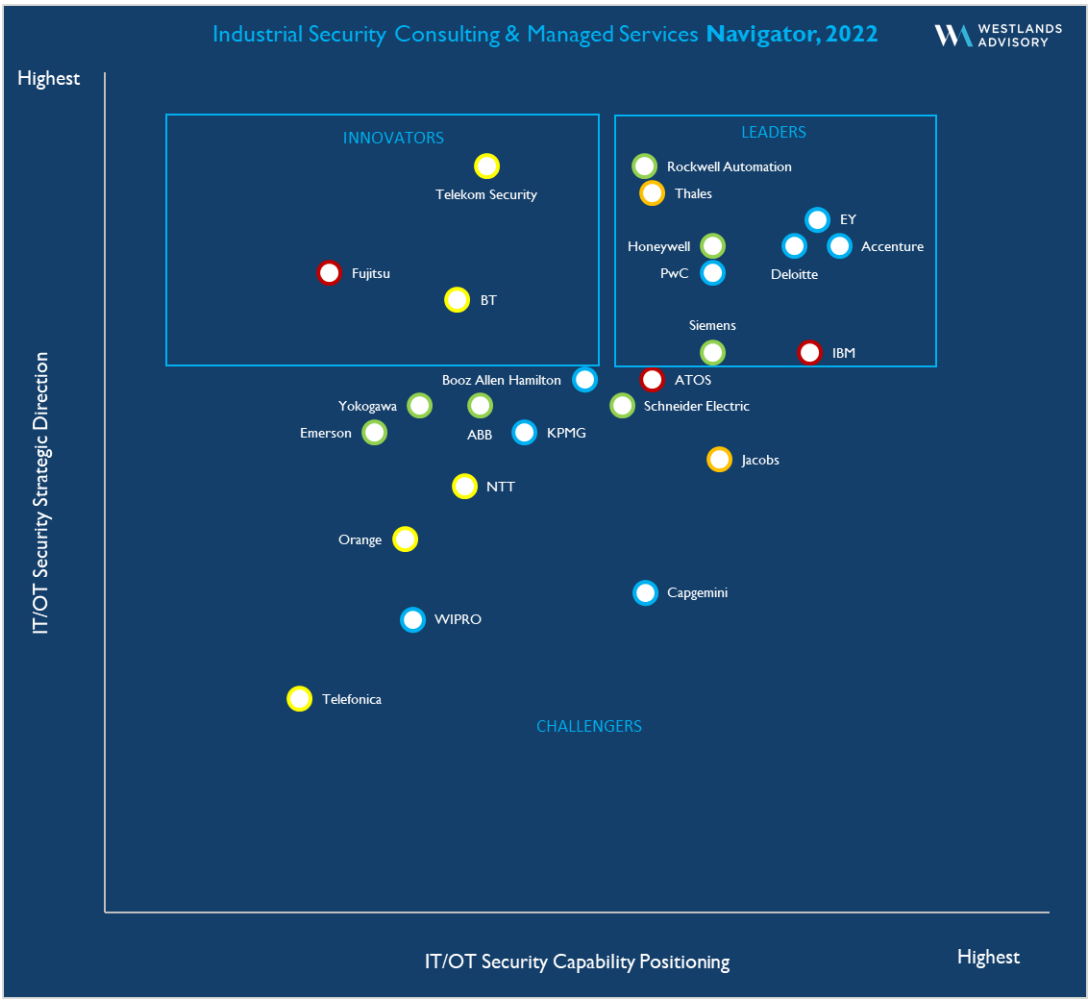
- *Governance & Risk Management* which includes the client risk assessment, standards adherence and creation of cybersecurity policies in relation to the business objectives.
- *Assessment & Assurance* to test the resilience of the operation and includes penetration testing, red-teaming exercises, and threat assessments. OT specific cyber ranges are used for both assessment & assurance, secure-by-design and staff training.
- *Advisory* services to overcome challenges. Use cases includes SOC operations, threat intelligence, incident response planning, remote access management, deploying new manufacturing processes securely, and staff training and awareness programs.
- *Secure-by-Design* to build cybersecurity into the engineering process to ensure that the product is safe and secure throughout its lifecycle. Use cases may include designing of sensors or machines for use within a manufacturing process.
- *Systems Integration* is the deployment of security controls and handover to the asset owner.
- *Managed Security Service*s providing remote monitoring and management of security through a single or networked set of Security Operating Centres (SOCs) usually providing a 24x7x365 service. This includes the controls and configuration management and threat detection. Advanced models include threat hunting and incident response that require the partner to have a strong understanding of industrial networks and processes. Incident response requires the partner to have a strong understanding of industrial networks and processes.

Industrial Security Consulting & Managed Services Navigator 2022

The methodology for the analysis is included below. The Industrial Security Consulting & Managed Services Navigator considers the global footprint of service providers, including offices, employees, support infrastructure and operations centres. WA notes that there are a significant number of Industrial Operators that are national with a localised supply chain. This includes for example many industrial SME (Small to Medium Enterprises) in Germany to large Utilities in Sweden, where regulation requires data to reside locally, to the many state level utilities in the United States. These companies are often serviced by highly specialised or regional firms that provide both the deep

industrial knowledge and localised support required. Regional focussed organisations are not represented in this analysis

The analysis considers organisations with knowledge of industrial control systems and the capability to advise, integrate, monitor, and provide support services, to the customer. Vendors that provide IT monitoring services to industrial customers without the capability to consult, integrate, and monitor threats to Industrial Control Systems are excluded.



- Engineering & Cybersecurity Services
- Professional Services Firms
- Industrial Automation Vendors
- IT Services Firms
- Telecommunication Service Providers

Innovator: Telekom Security

Summary

Telekom Security, a subsidiary of Deutsche Telekom (DT), is a leading Managed Security Services Provider in Germany, Austria and Switzerland (DACH) with the capability and infrastructure to provide customers with a global service. The organisation provides both professional and managed security services to commercial and industrial partners and employs over 1,600 security specialists.

The company is investing in several strategic areas to provide customers with the support and services to improve and protect business operations, including SD-WAN, Secure Access Service Edge and Industrial Control Systems security.

The Telekom Security industrial security operation is managed by its Security Operations Centre (SOC) in Bonn and supported by a further 7 located globally as part of its follow the sun strategy. This provides multinational manufacturing customers with 24x7 local support.

Positioning

Telekom Security's Operational Technology (OT) proposition is based on the company's knowledge and management of operating critical infrastructure, such as DT`s telecommunication network. The service portfolio stretches across the NIST framework, providing customers with an end-to-end industrial security service. The customer journey usually starts with an "OT Security Orientation Workshop" which identifies, quantifies, and prioritises current risks through asset inventory analysis, penetration testing and vulnerability assessments. Specific consulting services includes modules such as the "OT Security Strategy & Roadmap" and "OT Security Architecture", helping customers to design, build and manage a security process aligned to their risk program. This includes employee security training and awareness.

Telekom Security strengths include:

- Strong refence list across manufacturing and critical infrastructure verticals, demonstrating experience of delivering complex, global security solutions.
- Trusted brand, particularly in the DACH region
- A mature and wide range of services to meet a variety of use cases. This includes a strong asset discovery capability which links to OT vulnerability management and OT threat intelligence services. Passive collection and on-site investigation deliver a near 100% discovery rate.
- Significant experience of advising manufacturing and process industries on risk with experience of all industrial standards. This includes a growing team of professional security advisors with industrial experience. Internal certification and training programs ensure continual improvement of the staff.
- Advanced OT Services include Threat Information, Threat Monitoring and Threat Analytics. Strong proprietary threat intelligence consists of data collected from a variety of sources including DNS requests, over 900 honeypots, cloud services and OT SOCs.
- Global services including a network of SOC's with OT related services. Telekom Security's dCERT provides advisory on OT specific vulnerabilities.

- Ecosystem partnerships and strong working knowledge of industrial protection technologies including threat detection and vulnerability management. Telekom Security's strength is the implementation of technology into workflows including development of detection cases and run books.

Strategic Direction

OT Security is an important part of Telekom Security's growth strategy and therefore Westlands Advisory expects the organisation to continue to invest in improving and expanding OT related services. This includes further evolution of its managed security services and investment in consulting staff. Westlands Advisory also expects that services are likely to evolve to meet the specific requirements of industry sectors that have varying risk and compliance profiles, engineering challenges, and operational requirements.

Telekom Security currently provides an end-to-end industrial service across the NIST framework (Identify, Protect, Detect, Respond and Recover) for both IT and OT operations. This includes risk identification, advisory services, integration, and management of the security operation using automation and proprietary threat intelligence. To meet the growing customer focus on recovering quickly from a security incident, Westlands Advisory expects to see further investment in services related to incident response, business continuity management and disaster recovery.

Telekom Security is an industry thought leader and innovator which includes a focus on developing new business models, processes, and technologies.

- The Industrial Security Center, developed in collaboration with Hitachi Energy and Securitas, is a unique business model and service designed to protect energy operations. The solution includes shared intelligence and networking between the partners to ensure resilience across industrial, cyber and physical security operations.
- New techniques and methodologies to identify and manage assets.
- The company has a proactive role in the security industry across the DACH region which includes working relationships with government and regulatory bodies, regularly sharing knowledge on threats, vulnerabilities and best practices.
- Telekom Security also has deep vertical market knowledge. This includes the automotive industry where the company has considerable experience of the systems and processes related to supply chains, design, manufacturing, business operations and infrastructure.

Additional Information

Methodology

The research for the report was conducted from September 2021 to March 2022 and builds on earlier work throughout 2019-2021. The research process included interviews with vendors, CISO's and engineers, and a wide range of interviews with services providers including industrial automation, professional security services firms, and managed security service providers. Service providers were scored on the following basis.

- IT/OT Capability Positioning

    - 50% of scoring based on capability and operational examples aligned to NIST CSF
    - 50% of scoring based on assessment of 9 criteria (vision, services, culture, ecosystem, platform, business models, threat research, global, expertise)
- Strategic Direction
    - 100% of scoring based on assessment of 9 criteria (vision, services, culture, ecosystem, platform, business model, innovation, global, expertise)

Qualification

Organisations were included based on meeting the following criteria.

- Operational Technology expertise including people, OT specific SOC's and capability centres that includes cyber ranges.
- A wide range of services to support customers deliver against IEC 62443, NIST CSF and other relevant regulation or standards. This includes the ability to advise, integrate, monitor, and respond to incidents.
- Global capability with strong representation in more than two regions globally (NA, LATAM, Europe, Middle East & Africa, Asia)
- Strong set of customer references

Further Research

- Westlands Advisory's OT Security Industry Analysis 2022 (Released April 2022)
- IT/OT Security Platform Navigator (Released April 2022)
- Industrial Security Services Navigator (Released April 2022)

For further information contact info@westlandsadvisory.com

[i] Westlands Advisory's "Global OT Cybersecurity Industry Analysis"
[ii] SANS 2021 Survey: OT/ICS Cybersecurity
[iii] Ponemon Institute "The State of IoT/OT Cybersecurity in the Enterprise"