Industry 4.0:

Secure and resilient operational technology

Foreword

The 2022 Connected Industry Report reminds us that in a hyperconnected world, we must remain attentive to the ever-evolving cyberthreat landscape.

IT and OT environments are converging. The more connected devices you introduce into your environment, the greater your level of potential vulnerability and risk. This whitepaper outlines how businesses can build a secure and cyber-resilient OT environment covering governance, technologies, risks and threats, frameworks and approaches to be successful.

Gareth Watters is the Principal Cybersecurity GTM Strategist for NTT Ltd and has been working in IT and Cybersecurity for over 20 years.

Introduction

Industry 4.0 is evolving beyond the realm of manufacturing, opening new doors of possibility to organizations in other sectors. Now's the chance for businesses of all kinds to make step-change operational improvements, better compete in their marketplaces and uplift their communities.

We're living in a world of the Connected Industry.

But adopting a Connected Industry mindset and embracing the opportunities that come with it also introduce a new breed of challenges and risks, particularly as it involves a blurring of the traditional lines between operational technology (OT) and information technology (IT).

Security cannot be an afterthought in Connected Industries. All solutions and environments should have security and privacy by design embedded across all layers. The more devices you introduce into your environment and the higher the degree of interoperability between previously discrete systems, the greater your level of potential vulnerability and risk.

In this paper, we'll explore the path to secure IT/OT, precisely laying out the steps CISOs can follow to build an agile, risk-aligned cybersecurity posture that spans their organization's IT and OT environments.

We'll look at strategies and tactics to gain better and more advanced visibility of threats and vulnerabilities across both sets of infrastructure so you can protect, respond and recover more effectively.

Specifically, we'll look at how to formulate, execute and optimize an OT Security Governance Framework that will serve as the compass to guide processes, people and controls in a risk-managed fashion.

Read on to explore the path to operational resilience in a hyper-connected world.

Security cannot be an afterthought in Connected Industries. All solutions and environments should have security and privacy by design embedded across all layers.

What is Industry 4.0, and why do you need to secure it?

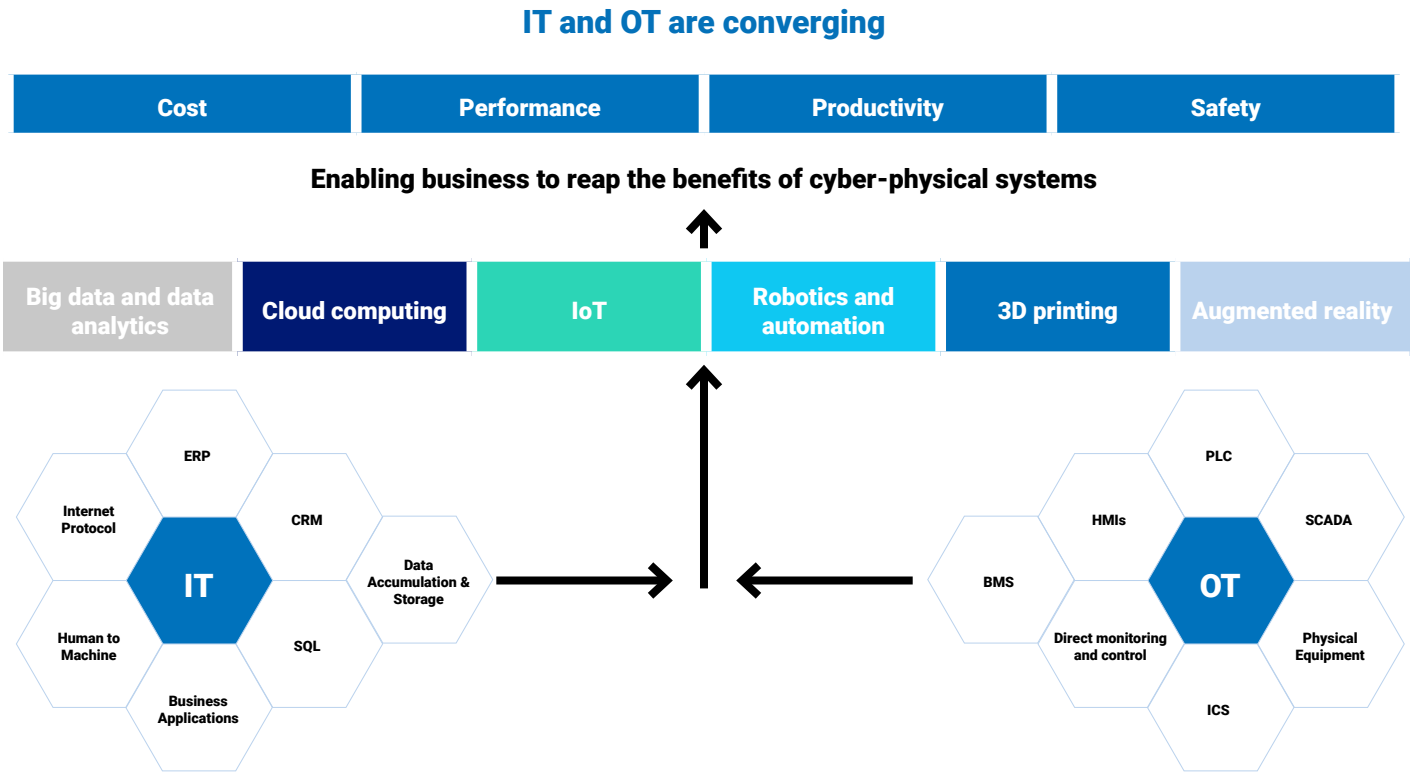
The term Industry 4.0 refers to the combination of several major innovations in digital technology all coming to maturity. These include public cloud computing, artificial intelligence (AI), robotics and cyber-physical systems (CPS) that are poised to transform all industry sectors in that they are part of a set of interconnected efforts. From smart cities, the Internet of Things (IoT) and the Industrial Internet of Things (IIOT) platforms to operational technology (OT) and critical infrastructure, they're all now living in a digital era. Industry 4.0 is, in essence, the digital transformation for industry, which corporate organizations have been undergoing for several years now. In order to deliver digital transformation within an organization, it requires both a network and a security transformation.

Industry 4.0 is allowing organizations in manufacturing, transportation, energy, utilities, retail and healthcare and more to make significant operational improvements, better compete in the modern world and better support our societies. Adopting a growth mindset and embracing the opportunity has its challenges and risks associated with it, but with careful planning, there are numerous business benefits to be unleashed in terms of profitability and becoming more agile. Also, being interconnected is saving (and generating) billions of dollars each year through efficiencies created by connectivity, insights, innovation and automation. Safety is also improving with the ability of machine learning-enhanced sensors and robotics improving the ability to ensure safe working environments. Our society is improved as industry digitally transforms with better utility services, healthcare and an improved food supply chain, e.g., fresh food with traceability from farm to plate and automated farming machinery, among some of the connected innovations.

However, the rapid introduction of new technologies across the OT industrial sector (e.g., manufacturing, utilities, mining, transport, oil and gas) has resulted in the convergence of the IT and OT environments. And now, Industry 4.0 is extending its reach into other sectors at pace.

Previously unconnected systems, devices, sensors, processes and tools that have existed relatively unchanged in OT environments for decades are now computerized and connected to network technologies, public clouds and the Internet. Likewise, IoT devices, which share some common functionality as OT devices such as sensors, actuators, meters, machine-to-machine communication and embedded systems are also being deployed in OT environments. Offline environments are now online and the technologies, e.g., industrial control systems used in OT environments require different security and risk management processes and technologies to IT environments in order to minimize cybersecurity risk. However, there are also several similarities between the tools and technologies that are used for IT security that allow them to be applied to OT security.

Industry 4.0 is allowing organizations in manufacturing, transportation, energy, utilities, retail and healthcare and more to make **significant operational improvements, better compete in the modern world and better support our societies.**



Technologies that are changing the game and the cybersecurity challenges they present

Advanced connectivity is an essential part of connected industries. It's a vital element for the adoption and success of other Connected Industry technologies such as automation and IoT. So, it's both a value generator and accelerator.

While the promise of 5G is alluring, many executives view integration with legacy systems and infrastructure as a key barrier to overcome for implementing 5G networks. Some of the security concerns pertaining to 5G are inevitable consequences of its benefits, although it doesn't fundamentally change what security is needed to protect assets and data. For example, a 5G network is a more lucrative target to cybercriminals since it has a greater volume of data traversing it. Malware could also be installed and distributed at a faster pace. Connection stability becomes increasingly important where 5G connections might be used for remote driving or in healthcare situations. Integration with legacy systems and infrastructure also poses challenges, including the introduction of vulnerabilities into the new environment. A CISO therefore needs to be able to detect vulnerabilities, threats and blind spots earlier and respond faster than ever before.

Private 5G networks offer a viable alternative. These are 5G networks that are deployed entirely on the enterprise site, with private spectrum being leased by the enterprise themselves. Private 5G networks provide advantages to industries in terms of speed, control, reliability and security. According to NTT's Private 5G Economist Impact CIO Report, Private 5G networks are expected to become the standard across industries as well as a critical part of operations, with just over half of the companies surveyed planning to implement a private 5G network within 6–24 months.

So why is Private 5G a more secure option? Essentially, Private 5G networks act as an extension of the enterprise LAN network that uses 5G technology to enable that extension and connect users and devices to that LAN. The network is completely under the control of the enterprise, and all data stays on site and all existing enterprise security policies and procedures are applied to the 5G network. This is in contrast to telecoms networks that are generally designed to support larger groups of users with diverse needs.

There are compelling reasons to consider a Private 5G network in industrial environments. First, they offer a means to add an additional layer of security to facilities. Not only is 5G inherently more secure than other, more traditional forms of connectivity such as 4G and Wi-Fi, it's also easier to integrate with more modern security technologies.

Industry 4.0 also centers around the ability to monitor large datasets, sometimes in real-time, from sensors in operational environments and make real-time decisions based on analytics and insights. The data collection, storage, processing and analysis are predominantly supported by services run in the public cloud. It's great to see in NTT's 2021 Hybrid Cloud Report that **61.6%** of respondents view security and compliance as the first consideration in vendor selection for hybrid cloud. It demonstrates that as cloud-first models begin to dominate, business leaders recognize the real cyber-risk. But unfortunately, for the vast majority, there's a huge degree of complexity and uncertainty in how to keep data compliant and clouds secure. Similarly, there's still doubt (at least in the minds of business leaders) as to who should own the security of what when it comes to the cloud, data and supporting infrastructure. The Shared Responsibility Model from the Cloud Security Alliance helps, but each vendor has their own slightly different take. It's ultimately the data owner's responsibility to ensure their data is secure and compliant with their requirements. Managed cloud services providers can take ownership of the responsibility for secure cloud architectures and help organizations to focus on getting the desired outcomes from the cloud without being concerned with developing an in-house cloud capability.

Furthermore, the COVID-19 pandemic has pushed organizations to prioritize operational resilience . The need to rapidly shift to a hybrid workplace due to pandemic lockdowns was felt globally. Many manufacturing businesses, for example, have had to scale back on the ground personnel to prioritize safety and introduce more new technologies (i.e., remote control to devices, VPN) to maintain productivity. This has brought about new challenges with hastily deployed remote access solutions that have not been adequately secured, introducing new threats to previously offline OT environments. This increases a business's overall attack surface with more users and data outside the manufacturing floor. Furthermore, it's required security agility not seen before – the need to scale, flex and change security to an evolving global situation.

In summary, CISOs in organizations with OT environments to secure have a difficult juggling act. They must embrace the concept of Industry 4.0 and the technologies that come with it – 5G, the cloud, IT-OT convergence. They must also be champions of digital transformation because the business fundamentally depends on it to remain competitive, pandemic or not. However, they must balance the need to support the broader transformation goals with risk management, helping their business to remain secure and employees safe and healthy, through a pandemic and beyond.

[1] *2020 Gartner Risk Management During a Crisis survey*

Risks and threats to OT environments

OT systems and critical infrastructure are classified as a form of high-value/high-consequence asset because they are core systems for value, revenue creation and, in many cases, support society's basic needs (water, electricity, etc). When OT systems and the supporting IT systems are interfered with or disabled through a cyberattack, the impact to operations and society can be significant. Financially, there also remains a cost to investigate and restore operations. In some cases, this includes the payment of significant sums in the form of ransoms and, of course, the loss of revenues while the systems are being restored. Other issues include the potential loss of future business due to reputational damage and lost trust.

The number one threat to OT and critical infrastructure are nation state actors who target and disrupt our critical infrastructure and supply chains. They may use a variety of techniques and tools to do so, but the difference here is that they're often well-funded, resourced and powered by political motivations. For example, in 2009, the Stuxnet worm was used to attack Iranian nuclear centrifuges. It was the first example of a nation-state using cyberattacks affecting to disrupt another nation's infrastructure. Then, in 2017, the NotPetya attack unleashed the Sandworm malware with the intent to cause disorder in the Ukrainian electricity utilities sector. NotPetya ultimately had a worldwide impact and it's widely attributed to state-backed operatives testing their cyberwarfare skills. Threat intelligence indicated that numerous similar iterations and attack techniques had taken place on the same electricity generation stations and circuit breakers. The attacks caused actual physical damage, which was difficult and slow to repair. Furthermore, they caused societal unrest and had potential to paralyze a country. Protecting OT environments from the threat of nation-state actors is vital to national stability.

Ransomware is the next biggest threat to OT environments. The Colonial Oil Pipeline, whose oil and gas infrastructure supplies 45% of oil used on the east coast of the US was crippled by a ransomware attack on May 7, 2021. It's suspected that a criminal hacking group was behind the attack (as opposed to nation-state actors). It should also be noted that while the initial attack vector isn't known, the cybersecurity attack targeted the business side rather than operational systems, implying that this was a more financially motivated attack (a ransom of 75 Bitcoin value at approximately $4.4 million USD was demanded and paid) as opposed to political, with the aim of bringing the pipeline down. That said, it did ultimately affect operations as Colonial Pipeline proactively took some operational systems offline to contain the spread and damage.

Industry 4.0 is allowing organizations in manufacturing, transportation, energy, utilities, retail and healthcare and more to make **significant operational improvements, better compete in the modern world and better support our societies.**

But the impact on US society was so significant that we saw stockpiling and queues at gas stations due to supply shortages. The United States Cyber Command (CyberCom) and the full force of the US three-letter agencies responded to the ransomware perpetrators by going after the ransomware crew, their infrastructure, people and ransom, resulting in the recovery of a large percentage of the ransom paid and several arrests.

In the same month, there was a further attack, this time on the food supply chain, with the world's leading meatpacker, JBS, having to shut down operations temporarily in the US and Australia, having detected an attack. JBS paid a ransom of USD 11 million and was back in operation within one day. The debate continues as to whether it's right to pay a ransom as this may highlight that you're a good target and willing to pay (or maybe insured) – which lends support to an unwelcome criminal business model. However, as these examples show, the opportunity for a successful ransomware haul exists and it remains a key motivator for criminal operators.

In a similar fashion to the Colonial Pipeline ransomware attack, on Feb 1, 2022, an attack on Houston, Texas based oil and gas company Shell revealed that it was re-routing oil supplies to other depots following a cyberattack on two subsidiaries of a downstream logistics firm. The logistics firm was hit with a ransomware attack that disrupted IT systems and the supply chain. It was being reported that this was a ransomware attack involving AlphV (aka BlackCat) ransomware. AlphV ransomware-as-a-service (RaaS) was first advertised in December 2021. Several overlaps between AlphV and BlackMatter and/or DarkSide have been identified, with the LockBit operator insinuating that AlphV has the same operator(s) as BlackMatter/DarkSide. Notably, DarkSide ransomware was used in the attack on the Colonial Pipeline in May 2021. As you can see, RaaS operations, which are advertised and sold on the dark web, continue to evolve even with the threat of national security services intervention.

The lifespan of operational technology is measured in decades, not years. Data leaked as a result of ransomware on extortion sites is likely to expose sensitive OT information – be it client data, business data or invaluable IP. For example, customer devices and addresses (e.g., utility meters), OT documentation outlining architectures, systems, passwords, employees, plant operations and projects allows global threat actors to complete the initial phases of reconnaissance, before orchestrating additional attacks, without ever having to probe the organization's network in advance. And, given the longevity of OT devices, the relevance of information leaked may stand for years following a breach.

As shown in these examples, responsibility for maintaining operations and critical infrastructure needs to be taken seriously by governments and businesses alike. As it's not if but when an attack will occur, it's important that governments and businesses are resilient in the face of disruption. Regulatory pressure on businesses increases as governments around the world continue to develop policy and legislation pertaining to the protection of critical infrastructure such as the Executive Orders (EO) Improving the Nation's Cybersecurity (14028) in the US and the Australian Critical Infrastructure Bill. Industry sectors also continue to develop standards for OT such as ISA62443 – Security of Industrial Automation and Control Systems (IACS) series of standards. Translating legislative and regulatory requirements into a manageable security program begins with top-down leadership with executive level support – we discuss the processes and ways organizations can begin to do this in the next section.

Given the longevity of OT devices, the relevance of **information leaked may stand for years** following a breach.

[2] *https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/*

Recommendations for OT cyber-resilience

For an Industry 4.0 CISO, the challenge of managing risk stems from understanding the security needs of both IT and OT environments as well as the evolving threat landscape as it pertains to their own business. With such a dynamic threat landscape across a greater digital footprint, CISOs must consider how they can be cyber-resilient in meeting the opportunities and benefits that digital transformation brings.

The nation-state threat to critical infrastructure as a first line of attack during a cyber-war, the threat from ransomware and the impact to operational resilience have confirmed that cyber risk isn't just an IT risk, but also an enterprise and national security risk. From a business perspective, identifying how the organization can continue to operate in the event of a material cyber event is now understood to be critical for long-term business success and, in some cases, as shown in the previous examples, important to society's stability overall.

Gartner defines operational resilience as a set of initiatives that expand business continuity management programs to focus on the impacts, connected risk appetite and tolerance levels for disruption of product or service delivery to internal and external stakeholders (such as employees, customers, citizens and partners). These initiatives coordinate management of risk assessments, risk monitoring and execution of controls that impact workforce, processes, facilities, technology (IT, OT, IoT, physical and cyber-physical) and third parties across the following risk domains used in the business delivery and value realization process: security (cyber and physical), safety, privacy, continuity of operations and reliability. Operational resiliency is tightly aligned to the outcomes of information security management.

The following are a set of high-level recommendations that define the framework within which operational resilience can be achieved (including cyber resiliency i.e., resilience against cyber-attacks) when managing the convergence of IT and OT.

OT security governance framework

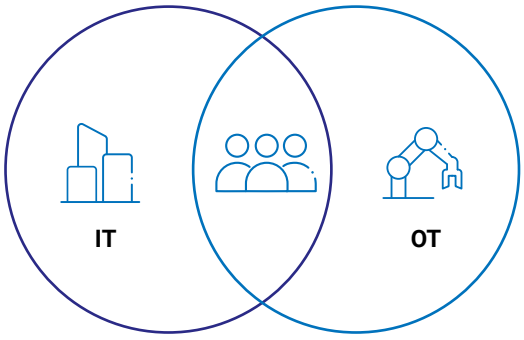
Operational resilience requires information security governance that guides the process, people and controls in a risk-managed fashion to protect the information, data and operations of an organization. To achieve information security governance, a CISO and must establish and maintain a governance framework to guide the development and maintenance of a comprehensive information security program. A typical governance framework would include the following key components:

- Organizational structure
- Roles and responsibilities
- A comprehensive strategy aligned to the risk appetite, IT and organizational business objectives
- Policies
- Standards for each policy-setting design requirements
- Institutionalized metrics and monitoring processes

To govern IT/OT convergence the information security governance must extend to include the OT organization in the form of an OT governance framework:

- **Organizational structure:** Implement a unified approach to information security governance across IT and OT by means of an executive-level steering committee that will be responsible for the strategy and planning. Support the steering committee with an advisory board of subject matter experts in both IT and OT.

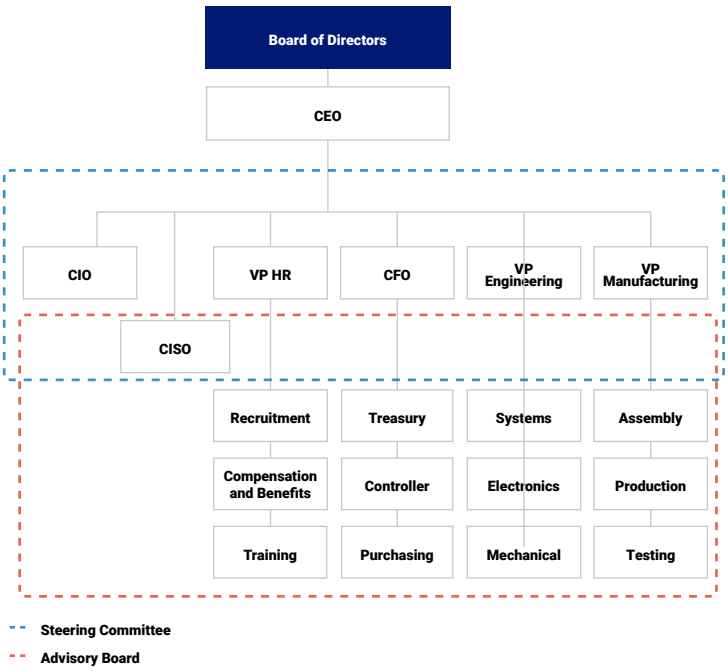
A Single Security Governance Body for IT/OT



Source: Gartner (January 2018) ID: 441788

A single security governance body for IT/OT provides a unified approach. The approach ensures visibility and governance at an executive level who are supported by the strategic advisory board of technical experts who span IT and OT. The IT\OT cyber security initiative should be led by an individual, either the CISO or a direct report Security Lead responsible for IT/OT security i.e at the convergence point of IT and OT and into the OT environment.

Typical Steering Committee and Advisory Board



Source: Gartner
ID: 441788

Source: Gartn

[3] *Gartner: Establish successful executive security governance in an integrated IT/OT environment*

Ensuring that the organization has a current set of clear standards supporting organizational policy **will ultimately improve operational resilience when it matters most.**

- **Roles and responsibilities:** With the correct organizational structure, the accountability, responsibilities and authority will be clear and unified at the top governance level. Clearly define a set of roles and responsibilities that outline the accountabilities and responsibilities across IT/OT in the development, implementation of the roadmap and for ongoing day-to-day IT/OT security. The alignment of the IT and factory/production/OT operations and risk and incident response resources will aid better cross-organizational workflows and security outcomes.
- **Leadership:** Assign a single IT/OT security program lead and functional team to deliver IT and OT security. They should focus on the standardization of processes, cross-skilling teams, removing duplication of efforts, implementing the security program that supports the security strategy and unification i.e., closing the gap between IT and OT functions.
- **Security strategy and security program:** Within a unified governing body, an organization can provide a common, executive lens to support the CISO when building a security strategy and program for IT/OT in an aligned fashion. A strategy will require a current and future state assessment and the development of a set of controls and processes aligned to the risk appetite and the regulatory, legislative and industry standard requirements. An Enterprise Architecture Framework such as SABSA (Sherwood Applied Business Security Architecture) or TOGAF (The Open Group Architecture Framework) provides a structured approach to defining resource relationships and process flows within a complex system such as an IT/OT environment. An enterprise architecture is recommended to ensure that conceptual and contextual elements such as business drivers and consequences are considered in the strategy development stage and there's a clear two-way justification and traceability possible between business drivers and security control decisions. Overall, an information security program generally includes a core set of common objective:
  - Maximize enablement of achievement of the business objectives
  - Minimize risk and loss related to information security issues across IT and OT
  - Support the organizational achievement of compliance
  - Maximize the program's operational productivity
  - Maximize security cost-effectiveness
  - Establish and maintain organizational security awareness
  - Facilitate effective logical, technical and operational security architecture
  - Measure and manage operational performance

A set of institutionalized metrics used for measurement will aid monitoring of performance and progress.

- **Risk management alignment:** Risk management alignment between IT and OT teams on the relevant IT/OT specific risks will benefit the organization under a unified risk management approach. Normally and prior to a unified approach, the risk appetite and methods to securing OT would be different to IT, with OT focussing on high-value consequences and safety and IT focussing on risks to the corporate side of the organization. A unified approach will provide tighter alignment between teams and improve the shared responsibility for securing the OT environment with IT tools and security controls, helping the broader business achieve its goals. Many elements such as safety of processes and for people will remain the scope of only the OT team.
- **Policies and standards:** Policies define the direction at the top level of the organization on what is acceptable as it pertains to the risk appetite. Standards further develop policies into specific instructions on what requirements should be in place to achieve the intent of the policy. Applying critical thinking to the organization's IT and OT security policies as a whole, especially with regards to business continuity, incident response and risk management, will provide a renewed focus on preparation for an event that may impact operational resilience. Ensuring that the organization has a current set of clear standards supporting organizational policy will ultimately improve operational resilience when it matters most. OT environments generally consist of multiple engineering and process technologies that are managed, serviced, and maintained remotely by third-party service providers, partners and contractors. Updating standards for system and vulnerability and patch management, data security as well as supply chain security will evolve the organization's approach to meet the present-day dynamic security requirements, focussing on the protection of sensitive intellectual property, secure remote access for employees, third parties, partners and contractors by identifying your critical assets and the methods of accessing and protecting them. The execution of the policy and standards will translate into logical (e.g. access control), physical (e.g. swipe cards), technical (e.g. firewall) and administrative (e.g. processes and procedures) controls that operationalize your IT/OT security strategy.

[4] *ISACA CISM – Certified Information Security Manager – Review Manual*

- **Management and operational alignment:** The CISO must execute upon the governance framework as a first step in aligning management and operational teams. With top-down leadership and endorsement, the alignment of management and their functional operational teams supporting the strategy must follow. This will be achieved through communication and sharing of information, processes and procedures followed by an analysis and development of new operating procedures that involve a converged IT/OT security approach. A product of the new governance model is alignment between risk, network, security and factory operational centres for better management, resourcing, collaboration, security and performance of teams within their domain as they support the convergence of IT/OT and key requirements for security, safety and operational resilience.
- **Institutionalised metrics:** When managing and measuring progress from the initial state to the desired state, one must determine what are the key indicators of success of unified governance, alignment to the IT/OT cyber strategy and alignment to the overall business strategy – and a more secure business overall. Industry frameworks such as the NIST Cybersecurity Framework (CSF), internal key risk indicators (KRI), key performance indicators (KPI), key goal indicators (KGI), etc., can be used to manage and measure progress. In the SABSA Whitepaper, the SABSA Governance Process, mapped to the four stages of the SABSA Lifecycle is an example of how an OT governance framework will look and function, and should be combined with a unified executive organisational structure and advisory board spanning OT and IT. Measuring success consists of defining measurable objectives, tracking the most appropriate metrics and periodically analysing the results to determine the areas of success and improvement opportunities.

A CISO must define the depth and breadth of metrics to provide information for management in a form of consistent reporting to promote the awareness of the importance that information security management has in the achievement of organizational objectives.

- **Culture:** When it comes to the culture change required to ensure OT security, the proverb 'it takes a village to raise a child' comes to mind. Top-down leadership, communication, training, awareness and collaboration throughout the organization will empower teams with the knowledge and tools to secure both the IT and OT environments and operational resiliency in the event of a serious incident. Having an advisory board supporting the steering committee broadens the level of support and buy-in from both business and technical resources and improves closing the communication and collaboration gap between IT and OT. Being an expert communicator and tailoring the message for the different parts of the organization will play an integral role in achieving the cultural mission.
- **Skills and resources:** A CISO will need a keen eye to identify the right talent to support the overall objectives. The ability to solve problems in complex systems, as well as think on their feet will be key to success. Surrounding oneself with the right team may be the difference between success and failure.

Working with a partner on OT/IT Security

While it's certainly possible to secure both your OT and IT environments in-house, working with a partner that specializes in security across both the OT and IT worlds can save you lots of headaches, time and money. Here are some suggestions as to when and where it might be useful to look to a third party for help.

- **Strategy:** Engage with industrial security specialists early to raise security awareness across executive teams and help align OT-specific business outcomes to IT/OT security strategy. Experts also simplify the process of assessing your business and aligning to complex government regulation and industry frameworks such as the NIST Cybersecurity Framework to ensure your organization is meeting its compliance and regulatory obligations and benchmarks for your industry.

A CISO must define the depth and breadth of metrics to provide information for management in a form of consistent reporting to promote the awareness of the **importance that information security management has in the achievement of organizational objectives.**

- **Incident response:** Incident response (IR) teams skilled in IT and OT incidents will assist in operational resilience planning and table-top exercises. IR teams can validate and provide robust policy and standards relating to business continuity management tailored to your organization. IR teams perform table-top exercises to test the plans. Having an IR retainer with a global IR provider ensures that when an incident occurs, you'll be their priority over all else.
- **Visibility, risks and gap analysis:** Specialist consultants can help to identify assets as well as gaps in the existing security architecture and security practices, identify security weaknesses, assess risks, prioritize areas for improvement, mitigate immediate risks and reduce the overall attack surface of your network utilizing ISA62443, NIST CSF and ATT&CK for Industrial Control Systems.
- **IT/OT architecture and OT security solutions:** A partner can identify, design and implement purpose-built solutions for industrial and process control environments that can scale to accommodate complex ICS and SCADA systems and provide full network visibility, control and protection for IT and OT protocols and, in some cases, secure remote access solutions. There are a number of vendors who specialize in this, and rather than building your own from scratch, it can be more straightforward to bring in specialists with the specific skills sets and tools you need.
- **Cross-platform capability:** Select a partner with expertise in Private 5G, networks, cloud transformation and acceleration and OT security to reduce risk and improve business outcomes. A partner with cross-technology tower domain expertise will ensure your transforming business remains continuously secure.
- **Threat detection and response:** Detecting threats across IT and OT starts with monitoring IT/OT convergence points. Typically, threat detection from the OT side involves monitoring for anomalies. The ability to detect and respond to threats in the IT and OT environment may provide a level of operational resilience and essential protection from a bad incident becoming a critical incident. Outsourcing threat detection and response further enhances the security operations team's ability to focus on optimization tasks.

In closing

While we've only scratched the surface of the topic of OT governance, risk and compliance, it's clear that engaging a partner with demonstrable global experience in the discipline of securing IT/OT convergence as part of an organization's overall digital transformation journey is a sensible move. Service providers that offer intelligent, platform-based services provide not only laser-focus and speed of execution, but also make your life much simpler. Automation of secure cloud infrastructure, network and workloads, security monitoring, detection and response will play a pivotal role in the CISO's mission of attaining IT/OT security.

Secure OT from NTT

Build an agile, risk-aligned cybersecurity posture that covers both IT and OT environments. Gain better visibility of threats and vulnerabilities across your OT and IT infrastructure to identify, protect, detect, respond and recover more effectively.

Read more

Bayer

Bayer brings its manufacturing operations' OT security up to date.

Read more

BW Offshore

BW Offshore cuts the risk to its IT and OT environments.

Read more


NTT