The Road to Digital Transformation: Enabling OT-IT Convergence

Authors:
Lorenzo Veronesi
Dominic Trott
Romain Fouchereau

IDC #EUR146160320

An IDC InfoBrief sponsored by
Situation Overview

Cybersecurity is one of the major issues affecting many companies

- Not only because cybersecurity threats greatly affect operations and put employees, society, and environment at risk
- But also because, though we can see a huge performance divide between digital and non-digital companies, the fear of security threats is preventing companies from exploiting their digital potential

To resolve these issues, cybersecurity must be put front and center in strategic decisions, as it is the essential enabler of digital transformation
Cybersecurity has a direct business impact, and the perceived risk is high. So why do security issues continue to populate the front pages, and what can be done?

The continued onslaught of ransomware has increased awareness of the disruptive nature of cyberattacks in IT and OT environments. We cannot ignore the risks of increased connectivity in OT environments, as the cost of production downtime and recovery caused by security incidents is steep. Due to the nature of OT operations, cyberattacks also create a risk of harm to the population and potential environmental disaster.

What is your organization’s greatest concern regarding a security attack?

- Equipment damage and downtime: 15%
- Financial loss: 30%
- Loss of intellectual property (IP): 16%
- Customer loss: 16%
- Reputational damage: 21%

Source: European Security Strategy Survey, Manufacturing sample, N = 67
Executive Summary

The Essential Convergence of IT and OT Domains

- The proliferation of natively-connected machines and IoT is creating unprecedented data proliferation and threats
- Securely connecting data across IT and OT domains is essential for information continuity to enable many business processes
- IT and OT integration has to be more than a “truce” between departments, but rather a converged and secure digital environment

The Journey Towards IT/OT Convergence is Not Always Straightforward

- Companies recognize that IT/OT integration is central to enabling new capabilities that lead to improved business targets, such as performance, reduced costs, and customer service
- There is no “one-size fits all” when it comes to integration models
- The complexities of IT/OT integration are difficult to tackle, and companies are still far away from real-time integration

Make Security Your Cornerstone, Not Your Stumbling Block

- Security is the key barrier; many companies are afraid to move forward with their integration
- External providers can provide significant support in this journey
- To win the digital game, cybersecurity must become the enabler of digital investment

Make Security Your Cornerstone, Not Your Stumbling Block
The Essential Convergence of IT and OT Domains
We have never had so much data. Operational equipment instrumentation has increased over the past few years, and plants are also getting connected. In other words, the success of future operating models is dependent on data management.

The proliferation of natively connected machines and IoT is creating an unprecedented data EXPLOSION in the OT space.

As connectivity is now pervasive, companies cannot pretend their plants and assets are separated from their IT systems. This also MULTIPLIES the attack surface and leaves critical operational processes exposed to unprecedented threats.

Companies with over 75% of operational equipment that has been instrumented, is on the rise.

In all your plants, what percentage of instrumented operational equipment is connected in the following ways?

Source: IDC WW IT and OT Convergence Survey 2018, Manufacturing, N = 326
Connecting Data Across IT and OT Domains is Essential for Information Continuity to Enable Many Business Processes

An organization becomes operationally intelligent when all activities are digitized to significantly enhance business outcomes. This should happen at the process level and in the way manufacturers operate with the ecosystem of suppliers, partners, and customers. For this to happen, companies must enable data and information sharing between IT and OT.

This has multiple organizational implications, one of the most important being the need for mandatory collaboration between different job roles, from C-level to operational leaders, to handle security by sharing practices and information.
Historically, IT and OT have been completely isolated kingdoms. IT/OT convergence goes beyond simple connectivity — it’s about creating an intelligent, designed, interconnected ecosystem.

Simply “connecting” the IT-OT realms

FROM Connectivity

The “truce”

Two Kingdoms

IT Hardware

OT Hardware

OT Data Acquisition and Control Software

IT Apps

OT Apps

TO Interconnectivity

A truly converged digital environment

COMBINED BUSINESS INTELLIGENCE AND INFORMATION SHARING

IT Apps

OT Apps

OT Hardware

Virtualization

Security-by-Design

IT and OT integration must be more than a “truce” between departments; it should be a converged digital environment, enabled by security-by-design. Security can be the driver towards truly actionable convergence and enable value-generating approaches.
The Journey Towards IT/OT Convergence is Not Always Straightforward
IT/OT integration goes well beyond simple asset management, and is central to enabling new capabilities, leading to business targets such as improved performance, reduced costs, and better customer service.

This is particularly relevant now. IDC predicts that the impact of IT/OT convergence will be significant in a multitude of areas.

**Operational Performance:** improved throughput/service reliability at same or lower costs

**Reduced Cost:** ability to share resources across IT/OT

**Customer Service:** improving service performance to customers (on-time and/or in-full deliveries)

**Improved Product/Service Quality:** responding more quickly to product/service issues, predicting issues

**Agility:** improved flexibility in adjusting production/operations according to demand requests

**Safety:** enhanced personnel and public safety in operations

**New Products and Services:** ability to support new products and services with connected assets

**Inventory Management:** optimizing inventory quantities, mix, and location

**Sustainability:** more efficient and clean operations or energy/resource management

**Asset Management:** improved reliability/availability of assets

Source: IDC WW - IT and OT Convergence Survey 2018, Manufacturing, N = 326

---

**ASSET TRANSFORMATION**

To reduce critical equipment failure, by 2024, 40% of manufacturers will use field asset IoT data to intelligently diagnose issues and resolve autonomously, improving planned downtime¹.

**INTELLIGENT EDGE — ENTERPRISE**

By 2023, over 50% of new enterprise IT infrastructure will be deployed at the edge rather than corporate datacenters, up from less than 10% today; by 2024, the number of apps at the edge will increase 800%².

**OPERATIONAL EXCELLENCE**

By 2021, 80% of all industrial companies will have merged operational data streams with enterprise data streams to support broader and more rapid operational innovation³.

**CULTURAL CONVERGENCE**

By 2024, as companies shift to more distributed decision making, 50% of industrial organizations will have flatter organization structures, more cross-functional collaboration, and fewer middle managers³.

---

¹ IDC FutureScape: Worldwide Manufacturing 2020 Predictions
² IDC FutureScape: Worldwide IT Industry 2020 Predictions
³ IDC FutureScape: Worldwide IT/OT Convergence 2020 Predictions
IT/OT integration is a priority for most manufacturers, and integrated organizational structures are on the rise. But there is no “one-size fits all” integration model

Which of these governance models most closely matches the structure you have in place in your organization today and in three years?

- **INTEGRATED**: Control and execution system investment decisions are made through a shared services organization, a center of excellence, or a corporate function. There is business as usual collaboration between IT and operational technology. Decision making about investments and priorities for operations is undertaken as a single unit.

- **COORDINATED**: Each facility/plant/delivery system makes independent investment decisions about technology for control systems, but execution decisions occur across multiple facilities, plants, or delivery systems, through a shared services organization, a center of excellence, or a corporate function. There is collaboration between IT and operations teams on a project basis.

- **SEGREGATED**: Each facility/plant/delivery system makes independent investment decisions about technology for its operational requirements through control and execution systems.

Organizations are increasingly connecting data from OT environments to data analytics repositories, and CIOs are beginning to make addressing OT security risks a boardroom imperative to maintain the integrity of data and avoid a cyberattack due to that connectivity. But the options companies are choosing to coordinate these initiatives are still quite varied.

Which statement best describes your organizational structure for IT and OT?

- IT and OT organizations are integrated with one executive leader
- Part of the IT organization is integrated with the OT organization, and IT and OT report directly to the same executive
- Part of the IT organization is integrated with the OT organization, but IT and OT have separate executive leadership
- IT and OT are separate organizations but they report directly to the same executive
- IT and OT are separate organizations with separate executive leadership

Source: IDC WW IT and OT Convergence Survey 2018, Manufacturing, N = 326
Despite all these efforts, integration happens more often through a batch or mixed approach, and companies are still far away from real-time integration, which is the true way to enable seamless data handling between IT and OT domains.

Which of the following best describes your organization’s approach to IT/OT integration?

- **Manual integration:** Our IT and OT system integration mostly involves manually providing data to systems as it is needed. **15.4%**

- **Batch integration:** Our IT and OT system integration mostly is through batch processing on a scheduled basis. **29.0%**

- **Mixed approach:** We have many integration approaches depending on the assets and business requirements. **41.1%**

- **Real-time integration:** Most of our IT and OT systems are integrated in real time. **14.5%**

Source: IDC WW IT and OT Convergence Survey 2018, Manufacturing, N = 326

The complexities of IT/OT integration are difficult to tackle, especially because of heterogenous factory environments made up of different types of machinery and connectivity with different standards. Security concerns among both parties also play a role, resulting in mistrust and resistance.

What’s at stake? Given increasing competition caused by digitization, manufacturers can no longer rely on old, traditional measures of success. A mature approach to IT/OT integration results in faster access to data with fewer resources and to improved uptime. Companies will miss out on this if they do not reconcile their clashing IT/OT cultures.

Overcoming the divide requires cross-functional collaboration, top-down leadership, and business-level oversight. An example of the former is moving experienced engineers from OT business units under the CIO/CTO hierarchy.
Make Security Your Cornerstone, Not Your Stumbling Block
Security is the key barrier, and many companies are afraid to move forward with their integration, but removing the security barrier can boost all digital programs.

What are the top 3 barriers to IT/OT integration in your organization?

- Concerns about the security of integrating IT and OT systems
- Technology issues/incompatible legacy applications
- Too many decision makers/organizational complexity
- Lack of expertise on how to accomplish integration
- Lack of budget
- Not enough familiarity with the concept of IT and OT integration across the organization
- Lack of business case for the initiative
- Not a high enough priority

Advancements in operational technology visibility tools will propel 66% of global industrial firms to adopt an IT-OT integrated approach to security monitoring by 2024.

External Providers Can Give Significant Support in This Journey

Despite cybersecurity being a massive hurdle for IT/OT integration and operational success, companies struggle to handle this issue internally, as dedicated budgets are scarce and people are too busy looking after day-to-day business. Therefore, third-party solution providers can support companies in their journey as they bring with them proven industry-specific delivery models and technologies.

What is limiting your ability to improve your cybersecurity capabilities?

- Budget constraints
- Operations resources are too busy on routine operations
- Lack of insight into security sensitive activities
- Skills shortages
- Juggling conflicting priorities
- Security team spends time maintaining and managing security tools
- High levels of demand for new business services
- Not enough integration in the IT infrastructure teams
- Fragmentation or lack of integration of security product portfolio
- Complexity working across multiple security dashboards
- Complexity managing multiple security providers
- Competing with cloud resources used/shadow IT

Source: IDC EMEA, IT Security Survey, Orange Business Services, February 2019, N = 61

What are/would be your motivations for using a third-party security services provider?

- Industrialized delivery models
- State of the art technologies and techniques
- Predictable costs
- Peace of mind — feel good factor
- Specialist capabilities
- Resource constraints
- Management directive — we have to use a third party
To Win the Digital Game, Cybersecurity Must Become the Enabler of Digital Investments

In revenue and profit performance, IDC Global Performance Index Analysis highlights a massive divide between digital and non-digital companies. Digital investments are paying off, hence the cost of doing nothing is huge. This is what an integrated security approach can do for any business.


Across the whole of manufacturing, the economic opportunity for digitally transforming core processes (source, make, deliver) is enormous. A significant contribution to these benefits will come from improvement in operational process.

The Manufacturing Insights Global Performance Index (GPI) tracks growth metrics from 800+ publicly traded global firms in the manufacturing and retail industries. The GPI tracks general trends in manufacturing and retail subindustries based on the performance of a sample of companies from those subindustries, and historical data in the index may be adjusted between quarters based on the addition or subtraction of companies in the index or company restatements of historical filings. Estimates by Reuters.

Source: IDC WW IT and OT Convergence Survey 2018, Manufacturing, N = 326
Digital transformation is not easy, as it is composed of many dimensions. Only with a powerful operating model enabled by information sharing and organizational alignment can manufacturers deliver a successful customer experience. Bringing security to the center can help to deliver digital initiatives.

The key DX TRANSFORMATION Dimensions

LEADERSHIP
- Business Ecosystem
- Business Model Innovation
- Organization & Cultural Change
- DX Planning & Governance

OMNI-EXPERIENCE
- Ecosystem Experience
- Continuous Innovation Orientation
- Platform Service Delivery
- Omnidimensional Marketing and Loyalty

WORKSOURCE
- Managing Talent
- Managing Sourcing
- Achieving Optimized Work
- Facilitating Organizational Culture

OPERATING MODEL
- Connected Product/Service
- Connected Assets
- Connected Processes
- Decision Making

INFORMATION
- Information System
- Data Discovery
- Value Development
- Value Realization

How should these five dimensions be integrated? Companies have to establish a clear vision that informs the whole digital journey (Leadership). People and information management is the glue that keeps customer-facing initiatives and internal process execution operating in synergy.

In particular, operations uniquely enhance the experience provided by the whole organization to their end clients.

Only with a powerful operating model enabled by information sharing and organizational alignment can manufacturers deliver the successful customer experience that is required to thrive in this day and age.
**Essential Guidance**

Despite the convergence initiatives in place, OT will remain very different to IT, and IT security teams will not be able to replace OT people and take over operations, but there is a very important need to create the right collaboration between teams to ensure the full success of any project.

**Put the right person in the right place** —
Information security needs to be addressed by a C-level executive whose job is to focus on strategy and governance. This guarantees the alignment of security strategies. A security strategy, encompassing alignment with an organization’s business goals and strategic direction is an imperative, without which organizational security is at risk.

**Adopt OT-specific security initiatives** —
It is now essential that manufacturing chief information security officers extend their company’s security strategy to encompass an assessment of the security status and threats of any operational environment. This means continued technical audits and monitoring of what is happening, the use of non-intrusive security assessment and monitoring tools, adequate time management facilities, robust preparation and resolution training before any incident can occur, and hardware, network, and software backups at every critical point.

**Don’t save too much on security** —
This is not the time to reduce the budget for IT security and compliance. It may take some time, and it may not be easy to initiate at first, but this is the only way that companies can minimize plant floor security threats and cope with this new wave of manufacturing risk. But using security threats and system vulnerabilities as an excuse for delaying operational transformation processes will just make it harder to reap the benefits of digital transformation.

Careful security management, including security-by-design, can be an enabler to make it possible to reach the true digital potential.
Orange – Trusted by its Clients as an OT-IT Partner

- **2,400** AI and data experts
- **2,200** Cloud experts
- **3,000** Multinational customers
- **2,100** Cyberdefense experts
- **2,100** Multinational customers
- **CYBERDEFENSE**

A global presence for local services

- Our teams are located in over **100 countries** ready to deploy and supervise your networks and digital solutions on a daily basis.

- **70 datacenters**

- **10 CyberSoc** that bring together expertise in threat analysis

- **16 SoC** around the world monitoring and responding to events 24/7/365

- **5 major service centers:**
  - Brazil, Egypt, France, India, Mauritius

Financial services
- Transport and logistics
- Natural resources
- Healthcare
- Smart cities
- Industry
About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Copyright Notice

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Custom Solutions information line at 508-988-7610 or permissions@idc.com. Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Copyright 2020 IDC. Reproduction is forbidden unless authorized. All rights reserved.