ARC WHITE PAPER

JANUARY 2020

Enabling Secure Industrial Digital Transformation

By Sid Snitkin

Overview

Digital transformation is changing the face of industrial operations. But turning this into corporate-wide benefits requires a resilient, integrated cybersecurity strategy.

Digital transformation today involves far more than just connecting IoT devices to cloud-based analytics. Industrial managers, infrastructure operators, and smart city leaders are testing myriad technologies and broad-based connectivity options. They can expect a variety of benefits. Enhanced access to IT, OT, and cloud data can reveal inefficiencies and bottlenecks. Mobile devices with augmented reality (AR) and digital twins can increase worker productivity and improve safety. Cloud apps and low-cost, IoT-connected devices can enable rapid response to competitive threats and easier adoption of new ideas. Analytics and machine learning can facilitate development of better operating strategies. Finally, new operational technologies and system architectures offer significant promise to improve maintainability, enable innovation, and reduce disruptions during system upgrades.

Digital transformation offers enormous opportunities for industrial managers, infrastructure operators, and smart city leaders. But full-scale adoption requires a comprehensive, resilient cybersecurity strategy that integrates IT, OT, IoT, cloud and mobile security efforts.

While these and other benefits are being proven in various pilots and localized efforts, full-scale adoption is often delayed by concern over the cyber risks of new devices and expanded connectivity. A resilient cybersecurity strategy that integrates IT, OT, IoT, cloud and mobile security efforts is essential to reap the full benefit of new technologies and cross-domain processes. It will also help companies address existing issues with cybersecurity strategies that continue to leave critical assets at risk of a serious cyber incident.

Industrial Digital Transformation Has Broad Impact

Digital transformation means different things to different people. While frustrating, this lack of clarity is unavoidable. Technology changes are happening across many fronts and business leaders are encouraging people to find creative ways to use them to improve performance. This fuels a continuous stream of new and novel use cases for cybersecurity professionals to defend.

We're seeing increased adoption of new technologies and broader connectivity across the industrial landscape. This impacts every business activity. Following is a small sample of the many ways that industrial companies, infrastructure operators, and smart city leaders are leveraging these capabilities to drive better performance and reduced costs:

- ***Health, safety, and environment (HSE)*** – Use of robotics and remote operations helps minimize the need for human operators in hazardous environments. Use of analytics, IoT sensors, and mobile devices help organizations better understand the factors contributing to safety incidents and unhealthy emissions and issue proactive alerts to at-risk people entering unsafe areas. Use of a variety of new building automation sensors, smart meters, and mobile devices helps reduce energy and water usage.

- ***Operations and Maintenance*** – Use of robots, autonomous vehicles, and additive manufacturing to implement new manufacturing strategies improves performance and flexibility. Use of expanded data collection and analytics help operations to optimize production, maintenance to predict emerging failures, engineers to reduce variability, and regulators to assess compliance. Use of mobile tablets, augmented reality (AR), and digital twins help improve the effectiveness of operators, inspectors, and maintenance personnel.

- ***Engineering*** – Use of geospatial information, analytics, and IoT sensors can improve the efficiency of oil field development. Use of expanded connectivity facilitates better collaboration and handovers among the many parties involved in capital projects. Use of IoT sensors on physical infrastructure, like bridges, makes it possible to identify structural problems before they turn into breakdowns and delays.

- ***IT*** – Use of cloud apps and infrastructure can reduce license and maintenance costs significantly. Use of edge devices to collect and process

information helps reduce communication costs and improve response time. Integration of transactional systems with cloud analytics enables more flexible user access to information and lowers support costs.

- ***Process Control*** – Deployment of new OT system architectures, like that proposed by the Open Process Automation Forum (a forum of The Open Group) offers the potential to lower engineering and implementation costs, ease system maintenance, improve security, and enable innovation. Leveraging of broad-based, secure connectivity enables more use of cloud apps, analytics, and AI solutions in process control.

Benefits Require Comprehensive, Resilient Cybersecurity

Digital transformation benefits are driven by disrupting the status quo and challenging sacrosanct views of how activities are performed. Successful initiatives alter traditional roles and processes, automate activities, and integrate workflows across siloed domains.

This creative, unconstrained use of new technology may be great for business leaders but can be incredibly frustrating for security teams. Well-defined use cases and comprehensive threat analyses are foundational tenets of effective cybersecurity strategies. Ill-defined projects and cursory reviews lead to insecure technology deployments and new pathways for attacks on existing systems.

Creative, unconstrained use cases and rapid adoption of new technology may be great for business leaders but can be incredibly frustrating for security teams. Security review policies and supplier guidelines are not enough to manage this situation.

Security teams have tried to control these risks with traditional methods. Many have instituted policies that require pre-deployment security reviews of every digital transformation idea. But the time and effort required for these reviews is unacceptable to business leaders, particularly when sign-offs are required from multiple, disparate security teams. Organizations have also launched efforts to establish digital transformation security guidelines for suppliers and system integrators, but they have also failed to ensure secure deployments. Project managers frequently (but often reluctantly) grant exceptions to avoid delays and additional costs for changes to normal vendor security practices.

Security Teams Need a New Approach

The technology flexibility that fuels digital transformation benefits is central to its security challenges. New functionality is being deployed across a wide variety of endpoints, including on-premise IT and OT servers, private and public cloud platforms, mobile devices, IoT devices, and network appliances such as edge gateways. Connectivity options are equally diverse. These include a variety of wired, wireless, and cellular approaches. Each has its own benefits and security risks, so security teams need flexible and resilient strategies to ensure that they are prepared to meet every challenge.

To deal with these issues, security professionals need to move beyond the status quo. Perspectives on security requirements need to be broadened and generalized. Security roles and practices need to be integrated and streamlined to enable efficient, thoughtful security reviews. Security technologies need to be standardized and enhanced to support end-to-end security regardless of how digital transformation efforts are deployed.

Integration Needs to Replace Siloed Thinking

Industrial organizations have traditionally viewed security from a siloed perspective. IT systems, OT systems, cloud, mobile devices, and IoT present unique challenges that require different security people, processes, and technologies. Benefits of managing similar technologies with similar security methods have been discounted in the belief that unique domain concerns and constraints take precedence. While domain differences need to be acknowledged, the inefficiencies and ineffectiveness of current approaches can no longer be tolerated. Too many OT systems remain at risk and security inconsistencies facilitate cross-domain attacks.

Digital transformation illuminates and aggravates underlying problems with siloed cybersecurity programs. Organizations need to adopt a more logical, functional view of cybersecurity and recognize that risks are the same regardless of where or how a cyber device is used. This kind of security management requires specialists.

Digital transformation illuminates and aggravates the underlying problems with siloed cybersecurity perspectives. Who has responsibility for a mobile device used within a plant that integrates information from OT, IT and the cloud? Who ensures the security of a building management system that connects IT applications with a variety of building automation systems, like elevators, lighting, and HVAC, as well as new smart access control and surveillance

systems? Even when one group is assigned responsibility, they often lack the resources and expertise to secure and manage every piece.

To address these critical issues, organizations need to adopt a more logical, functional view of cybersecurity and recognize that risks are the same regardless of where or how a cyber device is used. Every operation needs support from people with specific expertise in securing PCs, servers, cloud applications, networks, mobile devices, and embedded systems that underlie modern IoT devices. Experts in specific application areas, like OT and cloud, can provide guidance regarding the appropriateness of various defenses and practices. But security management is best left to specialists.

Building an Integrated Cybersecurity Strategy

Efficient and effective industrial cybersecurity requires a comprehensive strategy that includes a cross-trained team of cybersecurity professionals, a common set of security management processes, and a shared security technology portfolio that supports cross-domain management of endpoint protection, network security, and threat detection and response. Clearly, an effective, integrated cybersecurity strategy must address connectivity among domains.

Integrating Security People and Processes

IT and OT leaders from major industrial organizations participated in a panel discussion on IT-OT cybersecurity at ARC Advisory Group's 2019 Industry Forum in Orlando[1]. They shared their approaches for driving integration of IT and OT security people and processes. There was consensus that *people* represent the biggest cybersecurity challenge and integrated teams offer the best solution to this serious problem.

People represent the biggest cybersecurity challenge and is best addressed through integrated teams. Leading industrial organizations are actively pursuing integration of IT and OT security teams.

It's essential to build trust between IT and OT personnel. Encouraging IT and OT groups to collaborate to develop common metrics, standards, policies, and processes helps foster this trust. This reinforces use of common

[1] IT/OT Cybersecurity Convergence – Part 1, ARC Advisory Group, May 16, 2019

terminology; creates a shared understanding of risks, helps everyone recognize individual strengths, facilitates effective teamwork, and focus efforts on the issues that represent the most risk to the entire organization. Panelists also highlighted the importance of framing cybersecurity as a separate profession with cross-training opportunities to help recruit, engage, and retain the appropriate people.

Most panelists drove process integration through use of the NIST Cybersecurity Framework. The comprehensiveness of this framework and its general acceptance ensure that all domains were considered and all issues addressed. This helped them identify areas where common practices and technologies could be deployed and recognize where unique approaches were justified. The framework also provided metrics that were helpful in creating the critical measures needed to monitor and manage security across many different domains.

Integrating Cybersecurity Technologies

OT system constraints underlie many of the silo perspectives in industrial cybersecurity programs. Legacy assets and insecure communications create serious challenges that cannot be easily addressed with equipment upgrades. Defenders need compensatory solutions for assets that don't support modern endpoint protection and for old, proprietary protocols. Where modern cybersecurity technology is applied, operating constraints limit timely patching and updates. Concern about isolation restricts use of cloud-based tools and safety concerns restrict support from remote security resources.

Integrated cybersecurity technology strategies enable cross-domain correlation and filtering of OT alerts, use of advanced AI/ML security technologies, and threat intelligence. Common networking technology across IT, OT and cloud systems enhances defenses.

Integration efforts must acknowledge the challenges in OT security, but don't justify the proliferation of locally selected, incompatible technologies. Solutions used in IT environments can be tailored to meet OT restrictions. This enables reduced license and training costs, more efficient resource sharing, and better management of end-to-end security in digital transformation efforts that cross domain boundaries. Technology integration can also reduce the need for multiple solutions in certain cases. For example, use of modern next-generation firewalls (NGFW) can eliminate separate solutions that have been used to support network

segmentation, deep packet inspection, anomaly detection, and threat prevention.

Technology integration can improve OT security by enabling cross-domain correlation of alerts, use of threat intelligence, and better information sharing across the corporation. As OT leaders recognize these benefits, they may be more open to use of cloud-based security management tools and advanced strategies that improve security management efficiency and effectiveness.

Integrated Connectivity

Perimeter connections and pre-defined data exchanges were adequate to meet these basic needs. Following this approach for every digital transformation effort will significantly increase security risks and overwhelm networking and security teams. Organizations need to recognize the current situation and implement an integrated connectivity strategy that ensures end-end security of every communications pathway.

Connectivity between IT and OT systems has always been important to industrial organizations. Manufacturers need to share operating plans and production results. Infrastructure operators need connectivity to manage and monitor remote sites. Perimeter connections and pre-defined data exchanges were adequate to meet these basic needs. But the limitations of this approach are already apparent.

Incremental changes to links and local networks to support use of personal devices within facilities, share OT data with cloud systems, support remote users and systems, and so on have created a maze of inconsistently secured pathways that jeopardize OT and IT system security. Following this approach for every digital transformation effort will increase security risks significantly and overwhelm networking and security teams.

Organizations need to recognize the risks of the current situation and the need to address a wide range of emerging connectivity security challenges like 5G and containers. Implementing an integrated security strategy will alleviate risks today and in the future. Addressing all these connectivity pathways will require:

- A shift in access/identity control management from perimeter boundaries to "zero trust"[2] recognition of individual users, devices and applications

[2] Cyberpedia - What is Zero Trust?

- Enabling more granular, secure management of message flows based on dynamic policies that consider individual users, devices, applications, protocols, and commands
- Centralized, cloud-based, management of access control and firewall policies across all domains to ensure consistent, end-to-end security
- Physical networking appliances (such as NGFW) that can implement enhanced access/identity and dynamic policies to control message flows
- Rapid ability to isolate suspicious assets on a granular basis
- Virtual networking applications to ensure consistent connectivity management in IaaS cloud systems and virtualized systems

Industrial IT organizations are already implementing these ideas to protect data centers, cloud systems, and mobile devices. These solutions need to be extended into OT systems to help ensure consistent, end-to-end security of digital transformation efforts.

Conclusions and Recommendations

Based on ARC research and analysis, we offer the following recommendations for owner-operators and other technology users:

- Recognize that digital transformation is enabling myriad benefits and every organization will have to deal with the related security challenges.
- Integrate IT, OT, IoT, mobile, and IoT cybersecurity efforts to ensure that you have the resources and processes to support rapid deployment of new technologies and use cases, and a technology platform that enables efficient and effective cybersecurity management.
- Implement an integrated connectivity security strategy to ensure consistent, end-to-end security of new applications regardless of where and how they are deployed.
- Gaps in existing OT security strategies and policies add urgency to the need for change and solutions are available for a successful transition. The only roadblock to a secure future is the decision to act.

This paper was written by ARC Advisory Group on behalf of Palo Alto Networks. The opinions and observations stated are those of ARC Advisory Group. For further information or to provide feedback on this paper, please contact the author at srsnitkin@arcweb.com