White Paper

Operational Cybersecurity for Digitized Manufacturing: Emerging Approaches for the Converged Physical-Virtual Environment

Sponsored by: Fortinet

John Santagate Remy Glaisner Robert Westervelt

August 2019

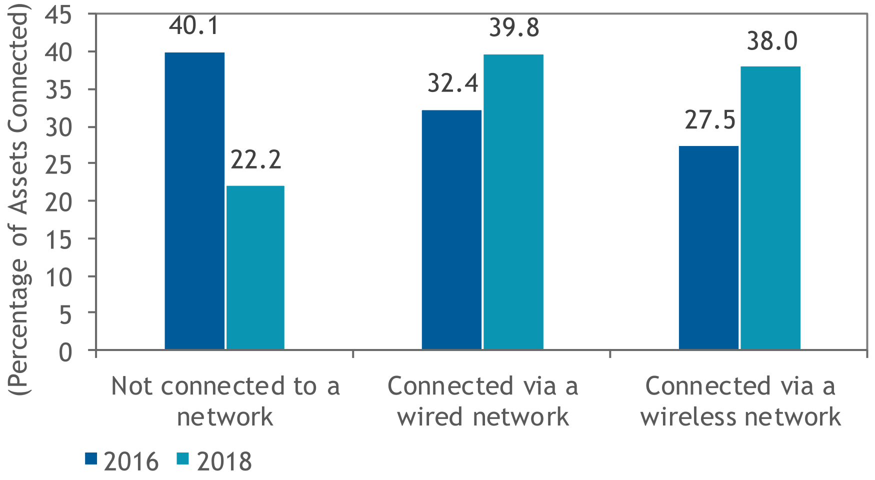
IN THIS WHITE PAPER

There can be no question that manufacturing environments are seeing a significant uptick in the ability to digitally connect their operation. However, for all of the benefits the proliferation of connectivity across the operating environment brings, it also increases risk. This prompts enterprises to extend their information security programs to improve defenses against cybersecurity attacks that threaten control and automation operations. This white paper explores how security-related issues are driving companies to develop and adopt strategies and a governance model to address the convergence of information technology (IT) and operational technology (OT).

In just two short years, the percentage of manufacturing operational assets not connected to a network decreased significantly from 40% in 2016 to just 22% in 2018 (see Figure 1). This significant drop in operational assets not connected indicates the shift in manufacturing operations to digitize. The increasing volume of connected operational assets is both a driver of the need for robust security to support converged IT/OT environments and a fundamental driver of the increase in data availability.

FIGURE 1

Evolution of Connected OT Equipment in Manufacturing



n = 794 (2016), n = 905 (2018)

Source: IDC's *IT/OT Convergence Survey*, 2018

Interviews conducted for this study revealed a variety of people and process hurdles that need to be addressed when organizations are planning to resolve cybersecurity risks within OT environments. Security teams must gain a clear understanding of what they are trying to protect before creating new policies and their accompanying enforcement mechanisms to an OT environment. The corporate operational intelligence leader at a global manufacturing giant acknowledged that his team is under increased pressure to better manage operational risk to digital infrastructure. Security policy is at the forefront of addressing this risk, and the most productive way to introduce security technologies into OT environments is for security to work with the frontline OT personnel to identify the most critical assets and the key points of risk. This approach is similar to the way IT security works with data owners and other business executives to understand the most critical assets and business processes that need the most protection.

"There's more of a recognition now than ever that there's a lot out there, and to do a good job, you can't just look inside the IT wall. It's unacceptable," the corporate operational intelligence leader told IDC. "When historically separate domains are connected, somebody has got to be accountable for the whole digital infrastructure."

IT security teams must understand the "real time" nature of many OT environments that have a significant impact on safety, production, or asset health. "When you do things like apply patches, if they're not tested, if they're not implemented with coordination and good communication, then you bring down production, and that costs money, or it can cost lives," the operational intelligence leader emphasized.

A chief information security officer (CISO) interviewed by IDC agreed that education and cooperation are essential for both IT and OT personnel to manage risks effectively in OT environments. Security can't and shouldn't have a disruptive influence on production. He noted that security needs to be an enabler and can't be too restrictive, or organizations could add risk rather than mitigate it. "One of the things we discovered is that for every security thing we had implemented, the [operations team] had implemented backdoors to go around it," the CISO told IDC.

It took the discovery of a targeted attack within that organization's OT environment to get OT and IT security personnel at the same table to address risks. The two sides agreed that security could help keep their manufacturing up and running and meet their deliverables and requirements in a more efficient way, he said. "There's never been a good way to address the vulnerabilities in their web interfaces and the underlying operating systems because it's all custom code … They tend to be the things that percolate up in our vulnerability management where we see a lot of at-risk devices in manufacturing. That's usually our most vulnerable environment, which is another reason behind trying to firewall and isolate it off from the rest of the network."

Overall, the increased dependence on digital connectivity across an operating environment is pushing the need for organizations to define a strategy for IT and OT convergence. To understand the implications of such convergence, organizations must have a frame of reference that uniquely defines OT and IT:

- **Operational technology** refers to the combination of technologies, systems, processes, and events that facilitate the control and automation of operations that are typically, but not always, in the physical world.
- **Information technology** refers to hardware, software, and peripheral equipment used to store, transmit, and analyze data and information. More commonly, IT represents the computer network of an organization.

Historically, IT and OT have been managed as separate entities within an organizational architecture, with some exceptions around reporting data and corporate networks. Now, with the cloud and connected operations becoming a standard architecture base for applications, operations (Ops) is suddenly feeling very exposed in its OT environment. New risks have caught the attention of security teams, CIOs, CISOs, senior management, and even boards of directors. For example, the air-gapped network of yesteryear is now riddled with holes as a result of this increased connectivity, which is further emphasizing the need for a robust approach to security at the OT level.

Three key points illuminate security issues in legacy operational technology:

- Weak cybersecurity capabilities in existing legacy OT platforms
- Undisciplined patching and version control of OT systems
- Belief that obscurity of the system to known threat actors is a significant barrier to access

As manufacturing organizations work to define their IT/OT convergence strategies, the increased vulnerability is defining the initial priorities of how IT and OT converge.

IDC MANUFACTURING INSIGHTS OPINION

Overcoming IT and OT Friction

Across industries, organizations must embrace the notion of IT/OT convergence, but they must do so with an understanding of the risk involved in extending the connectivity of the operation. This is especially true in manufacturing, where the top objective of the operation is to safely optimize productivity and throughput while maintaining continuity of operation. This objective is at odds with the objective of IT security, where one of the key points of emphasis is on information security to maintain data integrity and protection.

For manufacturing, the deployment and use of digital assets and the instrumentation of legacy assets with digital capabilities are done to enhance the ability of the operation to perform, via greater insight into the equipment and processes. Downtime can be extremely expensive. For example, consider the following hypothetical scenario:

> A plant running at an Overall Equipment Effectiveness (OEE) of under 80% for most of its assets, a 4% scrap rate, labor rate of $X/hour, and running at 80% capacity. Under this scenario, a reasonable expectation of the cost of unplanned downtime is 1.3% of sales per shift.

While this is a hypothetical example (built upon practical experiences), it helps showcase how unplanned downtime can have impacts on an operation upward of hundreds of thousands or millions of dollars per hour. The impact of unplanned downtime is a top reason manufacturing operations often turn to connecting their assets: to gain the data required to engage in predictive maintenance and reduce the impacts of unplanned downtime. A further driver of adopting connected operational assets is the ability to drive efficiencies in the manufacturing process. The data that is captured can significantly improve the ability to identify opportunities for improvement and drive out inefficiencies in the processes.

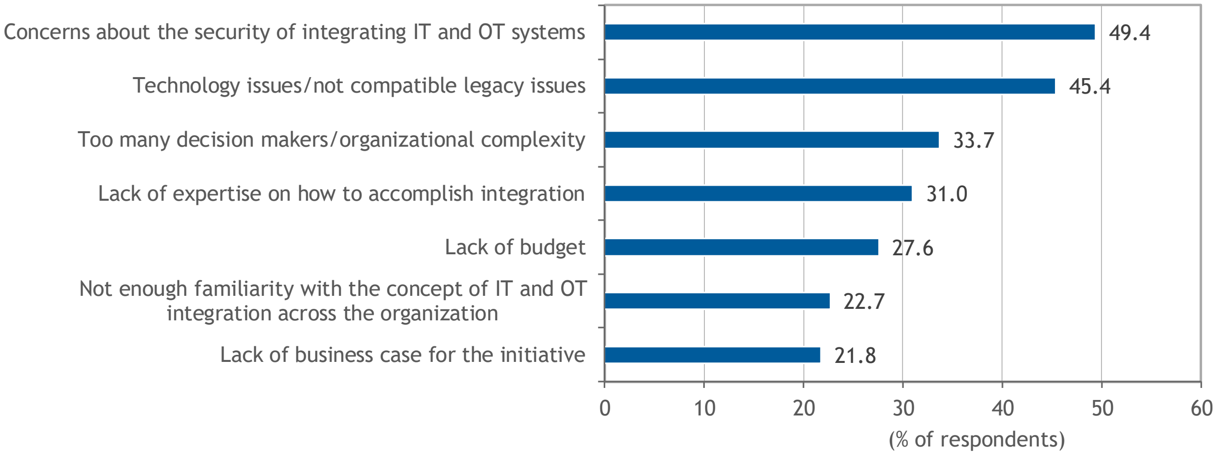
The IT organization, on the other hand, has worked vigorously to enact data security policy and procedures aimed at reducing cybersecurity-related threats. The average cost of a data breach is significant; an IBM study found the global average cost of a data breach to be $3.86 million, but in the

United States, this average jumps to over $7.9 million. Given this significant impact, IT-related security holds a long-standing perception of being rigid and designed to constrain the ability to accomplish malicious activity but also designed for rapid identification, response, and mitigation should a security breach occur. However, the operations side of the manufacturing organization typically covets flexibility and agility as sought-after characteristics. Operations is most interested in being able to adapt to change and leverage the tools it needs to develop the most efficient manufacturing processes. A significant risk exists when IT places highly restrictive security policies in place, prompting operations to pursue workaround alternatives.

An examination of the objectives of the IT organization and the operations side of the business reveals some competing objectives, which result in divergent priorities. However, the notion of converging IT and OT is about finding a way to address the divergent priorities while safely enabling the best of modern technology capabilities. As manufacturing organizations seek to engage in IT/OT convergence, they must look for ways to overcome the biggest impediment to enacting IT/OT convergence: the issue of security (see Figure 2).

FIGURE 2

Impediments to Enacting IT/OT Convergence Efforts by Manufacturing Industries



n = 905

Source: IDC's *IT/OT Convergence Survey*, 2018

Effectively addressing the IT/OT convergence security challenge means that manufacturing organizations must recognize the concerns from both the IT side of the equation and the OT side of the equation. These two sides of the organization must work together to create a security strategy that not only enables operational continuity but also maintains a digitally secure environment. IT security personnel must be open to enabling the flexibility required in the OT environment without being too restrictive or an impediment to production. Meanwhile, OT personnel must view cybersecurity as a necessary component of achieving business value and creating trust with customers. According to an operations leader at a global, diversified manufacturing organization, "There is a lot of education that has to go both ways … A lot of the IT group is accustomed to working in an office environment, and when you're in production, it's different, as it's real time and activity has immediate impact."

Taking on the IT/OT convergence journey is a collaborative effort. Neither the IT side of an organization nor the operations side of an organization can singularly and effectively design, implement, maintain, and secure a more robustly connected environment. This truly is a scenario where IT and operations not only will have to spend an appropriate amount of time and effort working together but also must be aware of the similarities and differences in terms of the way in which each of their respective sides of the organization accomplishes business.

SITUATION OVERVIEW

IT/OT Convergence Security-Related Drivers and Complexities

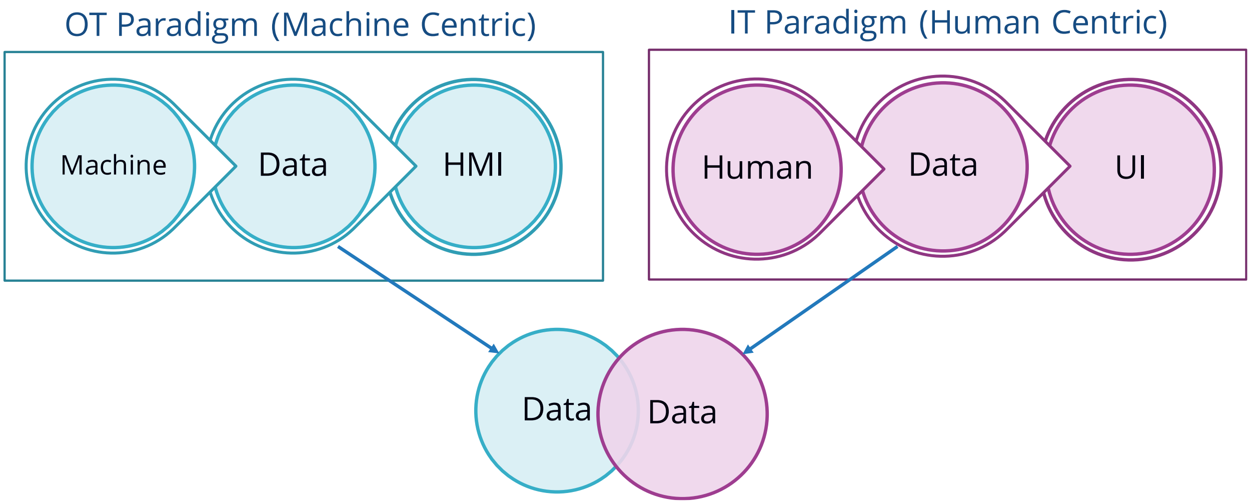
When one looks to understand what is driving organizations to invest in IT/OT convergence efforts and defining the complexities in doing so, it is useful to have an understanding of the common thread between the IT side of the business and the OT side of the business.

Data

Data is the common thread that brings alignment to the efforts to enact IT/OT convergence. The data may have a different source, may be different in terms of its meaning and impact, and may be used in a different way, but the common thread that brings IT and OT together is data (see Figure 3).

FIGURE 3

Data — The Common Thread Between IT and OT



Source: IDC, 2019

Across any organization, an immense amount of data is being created and captured specific to the operation. This proliferation of data is viewed as a gold mine of telemetry that can be analyzed to reduce costs or increase business value by enabling management to improve or create new products and services. From the OT perspective, this data is generated by the equipment and processes that are in use during the course of the day-to-day operations and primarily created by machines. From the IT side of the equation, the data is often human led; yet while the sources of the data are different, they must be considered as part of the overall digital infrastructure of an organization. Each data set on its own is useful and has historically been useful, but the value of the data when not aligned with each other is limited to its impact within the traditional operational silos. With IT/OT convergence, the idea is to bring these data elements together to enable a broader base of operational value built upon the information that an operation has about itself.

Given data as the common thread, the need to maintain an appropriate approach to data security must now extend beyond the IT domain. IT security is well understood to have a strong set of policies and standards that have been enacted to maintain IT network security. These policies and standards have been refined, implemented, and maintained at the IT level for many years. However, data-driven security policies, procedures, and standards are not so widely deployed nor understood relative to the OT domain. The rather recent increase in connected operational assets is both a driver and an impediment to enacting more robust security policy within manufacturing operations.

The Rise in Ad Hoc Connectivity

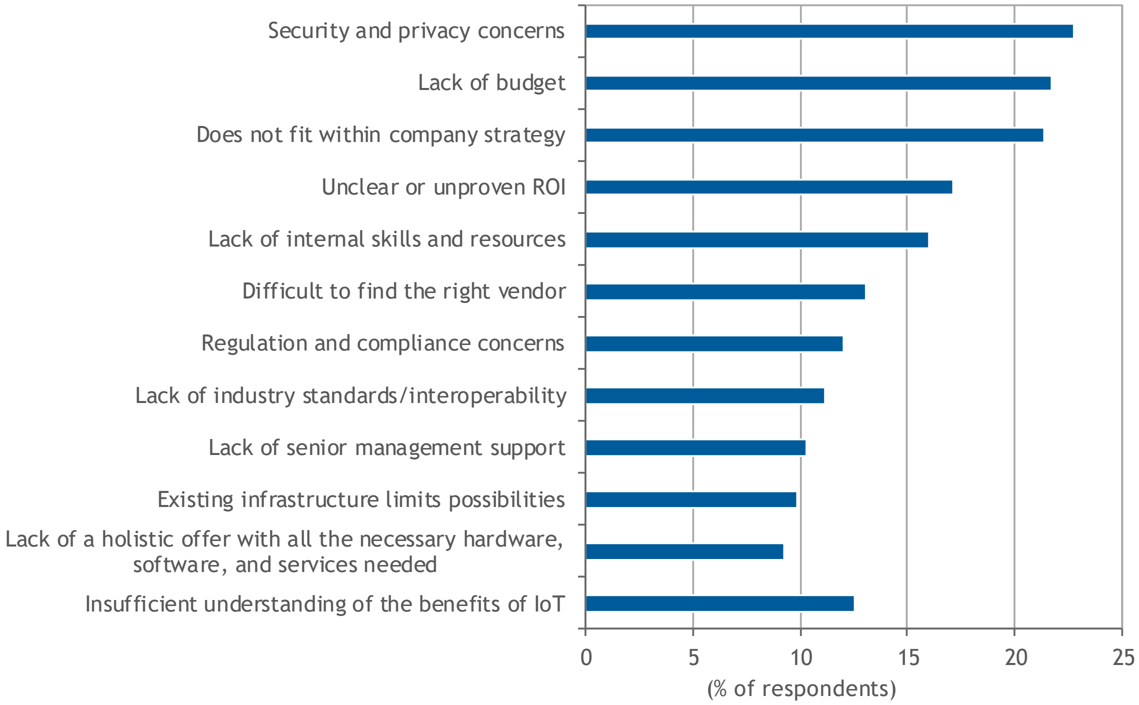
The increase in connectivity across operations is not something that has occurred strictly due to integrating new equipment that is built for operations in the current digital era. Most manufacturing environments rely heavily on legacy assets that are being connected through the increased deployment and use of add-on sensors that enable IoT connectivity to what would traditionally be a nonconnected device. Such an approach introduces an abundance of endpoint vulnerabilities to an operational environment. When an organization conducts a greenfield build of a plant or operational facility, it is much easier to deploy the latest and greatest equipment and technology. A greenfield build affords an organization a much greater degree of control over the ability to make use of modern technology, which also supports the ability of the IT organization to influence the technology deployed.

In reality, most organizations leverage operating facilities that have been in use for decades and thought to still have many more decades of useful operation. Such facilities pose a more complex problem when looking to connect the operation and engage in IT/OT convergence as the complexity involved in connecting legacy equipment and plants extends into the domain of security. The problem is, the widespread availability of sensors and connected technology is enabling local engineers to consider solving local problems by connecting their assets and working to make better use of the data from the operation, thus introducing many new vulnerabilities into the operational network. While such an approach is in line with the notions of digital transformation and modernization, when executed without appropriate checks and balances, it opens up the entire organization to the risk of malicious network access. The challenge of operations identifying ways to work around security policy was noted in IDC's interview with the senior infrastructure security architect for a global electronics manufacturer. When speaking about pushback to rigid security policy, he said, "Traditionally we've had quite a bit of pushback. In fact, one of the things we identified during discovery is that for every security thing we had implemented, they had implemented backdoors to go around it!"

Indeed, the security risk of connected operations is the leading reason that some organizations have chosen not to implement or invest in IoT projects (see Figure 4).

FIGURE 4

Reasons for Not Investing in IoT



n = 706

Source: IDC's *Global IoT Decision Maker Survey*, 2019

Of course, the security concerns around connected operations is a valid issue. Significant breaches have occurred for environments as simple as a connected HVAC system. For example, a major breach at Target happened when the HVAC monitoring service for one of its sites was hacked. Unfortunately, organizations opting to avoid modernizing their operational environments due to the security risk are likely also putting themselves at a competitive disadvantage. Rather than avoid engaging in IoT and connected operations efforts, organizations would find it far more beneficial to invest in collaboratively developing security policy that will allow for the use of modern technology while helping minimize the risk associated with connectivity.

Adapting to Evolving Threats

The digital threat landscape is not something that can be addressed at any one point in time and considered done. The constant patching and updating that are often conducted in the IT domain are executed because the threat landscape is not static. New viruses, malware, hackers, intrusions, and so forth are emerging on a continuous basis. Threats are ongoing and come in many shapes and forms. Furthermore, bad actors that exist are relentless and continue to advance their own skills in order to keep up with advances in security technology. While the same is true relative to securing an operational environment, the risk can actually be somewhat different and, in some cases, much more severe.

For both IT and OT, data security is about five key elements, albeit in different orders of priority and for different reasons (see Table 1).

TABLE 1

IT Versus OT Security Priority

IT Security Priority	Description	OT Security Priority	Description
Confidentiality	Information can be read only by the appropriate parties.	Availability	Assets and information are available for use by the people, assets, and processes that require them.
Integrity	Information retains its distinct content, and any changes can be identified.	Integrity	Information retains its distinct content, and any changes can be identified.
Availability	Information is available for use by people or resources that require it.	Productivity	Information and assets are available to operate as necessary in order to efficiently produce operational outputs.
Productivity	The use of computing resources that do not process sensitive information or data and yet provide value through its functionality.	Confidentiality	Assets and information can be accessed only by the appropriate parties.
Propriety	Protecting against the abuse of computing resources for inappropriate or otherwise unauthorized activities is key.	Propriety	Protecting against the abuse of operational assets for unauthorized activities and access is key.

Source: IDC, 2019

Regardless of how the policies, procedures, and equipment are constructed, these elements hold true for IT and OT related to security.

With the increase in connected equipment, the risk of a malicious actor taking control or changing the activity of an operational asset becomes a very real threat. This is especially true for operating environments that have taken it upon themselves to deploy connectivity capabilities throughout the operation without properly notifying the IT security organization and instead engaging in "shadow IT." Furthermore, the risk present within the operation itself now extends into the IT organization. Organizations that extend the connectivity from the operation into the IT organization for data storage, analytics, and retrieval create a direct access link between the operation and the IT infrastructure.

While IT infrastructure can typically be secured through firewall and client-side security applications, the same is not as true for the operations side of the business. Certainly, firewall technology is proven, but given the extensive deployment of IoT-connected assets in an operation, security in a converged IT/OT environment must be more segmented/layered as well as flexible. The requirement of flexibility is what really drives the need for a segmented and layered approach. Considering the divergent objectives between IT and OT (security/integrity versus continuity of operation), with a segmented approach to network security designed into an operational environment, a degree of flexibility can be accomplished without putting the broader organizational infrastructure at risk. Indeed, in the most sophisticated environments, there will even be production line-level security segmentation.

Beyond the preventive technology-driven security measures, there is also the element of physical security and processes to consider. For example, many IT organizations have policies restricting the use of nonapproved flash drives within a facility. This same example can hold true in an operations environment. However, when this policy introduces latency or impedes the ability to achieve efficient operations, the rationale for acting in violation of such a policy is heightened. Furthermore, it has become incredibly common for operations engineers to experiment with connectivity deploying capabilities such as Raspberry Pi. These devices are inexpensive and quite simple to use, and they enable flexible connectivity to operational assets. These devices introduce further risk because they are not secure, yet they are connected to operational assets and being allowed to communicate on the network.

Converging Technologies, Diverging Maturities

Given the maturity of IT security, operations traditionally depended on IT's network perimeter defense to secure OT. Little effort was made to secure systems with that perimeter in place. IT has matured its cyberstrategy to system and device security, while OT has lagged in terms of security because of the IT security blanket.

At this point in the technology evolution, it is OT's turn to mature. Engineers are developing instrumentation systems on board-level computers such as Raspberry Pi. As these devices are deployed, there is little thought to system security because these devices are installed on the plant network. Such actions introduce significant points of vulnerability. In fact, there are documented cases where these systems have been the focal point of security breaches once the corporate network's perimeter is breached. For example, a report by the NASA Office of Inspector General revealed that 500MB of data related to Mars missions had been stolen in April 2018. The source of this breach was an unauthorized Raspberry Pi connected to the NASA Jet Propulsion Laboratory.

OT must seek to leverage IT best practices as it develops its new security operating model on system and device security but must also adapt these best practices with modifications appropriate to the priorities of the operating environment. Given the more mature state of IT security, OT can learn a lot about what has worked in the IT environment. This does not imply that IT policy can be dropped into an OT environment; rather, OT must engage with this element of the business to leverage the lessons learned and best practices as it builds out its own approach to security. At the same time, IDC has found that CIOs are under a mandate to not slow innovation in the plant. IT and Ops must practice a governance model that doesn't inhibit innovation while minimizing the vulnerabilities that often accompany that innovation.

FUTURE OUTLOOK

The increase of connected operational assets is introducing new sources of risk for an organization, and firms are working to mitigate these risks. As operations increasingly look to enable connected operations and build out security for these environments, it is imperative that they look to innovate their approach to security for the converged IT/OT environment. IDC sees the future operational environment as one that can be described as a centralized operations performance management (OPM) model.

The OPM behaves like a NOC where all network/process operations are monitored and issues are diagnosed. But it also follows an IT model for asset, process, network, and device management. Just like IT, assets and nodes that are suspect can be quickly isolated and addressed. New assets and processes can be rapidly or automatically provisioned and validated to operate on the network and in the operations. The connectivity of the assets and processes is continuously monitored for optimal operation. Data integrity and validity are monitored to maintain trust in the data as it is analyzed and fed back into the process.

This converged IT/OT OPM structure is staffed initially by Ops, IT and, most likely, asset OEMs. But as the concept matures, the IT and Ops staff will begin to blend. At some point, the OPM center will be staffed by Ops/IT hybrid personnel and OEM experts. And just like within a modern IT organization, decisions on what are critical in-house operations and what can be outsourced as more commodity operations can be made effectively.

Under such a model, the role of OT security is also built into the OPM given that the network is ultimately run through the OPM center. The vision for the model is one where centralized management of operational data drives efficiencies in process yet also enables a more nimble operation. While this model is quite forward looking, the technology landscape is evolving to a point where such a model becomes feasible and likely the future approach to managing operations in the digital era.

ESSENTIAL GUIDANCE

There are many reasons that OT organizations are continuing to invest in connecting their operations. These reasons blend between business-related drivers (reducing cost, improving productivity, gaining efficiency, etc.), availability of new technology, and ongoing modernization. However, increased reliance on data, proliferation of connectivity, and divergence between IT and operations priorities are really driving the emphasis of security as a key IT/OT convergence element. As operations continue to look for ways to gain business efficiency, through digital connectivity, cyber-related risks will continue to be a focal point.

It is not a matter of time before some intrusion or malicious event occurs; rather, it is how impactful the event will be and how quickly an organization will be able to recover. Organizations that bring together the IT and operations sides to collaboratively define the appropriate security policies will most certainly find themselves better equipped to maintain high levels of security even in an increasingly connected operation.

For operations leaders looking to develop a security strategy designed for a converged IT/OT environment, IDC offers the following points of guidance:

- Make the development of the security strategy a collaborative effort involving representatives from both the IT organization and the operations side of the organization.
- Do not rely explicitly on traditional IT security policies when building out a security strategy for an operational environment. While IT policies can provide a good starting point, the conflicting priorities between the IT organization and the operations element require security policies that align with the priorities of operations.
- Consider the risk of operational workers building "workarounds" when their needs do not align with security policy. Build into the policy a way to mitigate and resolve these types of "shadow IT" issues.
- Continuously monitor the state of the security market. The threat profile is constantly evolving, and the bad actors are maintaining a relentless pursuit of vulnerabilities.

Companies that define their OT security strategy aligned with the digital strategy of an organization will be better positioned to minimize the occurrence and impact of security-related threats. The connected nature of the modern operation requires organizations to rethink their approach to digital security, specifically as it relates to the operation and OT. Organizations must embrace the growth of connectivity because there is much value to be gained. Likewise, the increase in vulnerability must be equally embraced, and companies must craft security strategies that are effective for the threats of today and agile enough to evolve to meet the needs of tomorrow.

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.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.