New York Law Journal

# Beyond Data: Function Is the New Cyber Attack Surface

**The profound changes deriving from IT/OT convergence require us to take a fresh look at legal and regulatory norms that have stood for decades since the Industrial Era. We are in a radical new environment where exponential benefits and risks are now reality.**

By **Edna Conway** | March 01, 2019

Imagine a hacker, armed with nothing more than a laptop, taking down the power grid, leaving millions without running water, refrigeration, lighting, access to money, technical devices, and eventually food and medicine—for weeks, or longer. This scenario is far closer to plausible for all manner of critical infrastructure because the long-predicted convergence of Information Technology (IT) and Operational Technology (OT) is now reaching critical mass.

The interlock of these two traditionally distinct technology domains is both logical and inevitable in today's increasingly digital world. IT is enhancing the feature sets, efficiency and operations of the OT infrastructure that runs both enterprises and nation states. While this convergence of technologies brings significant benefits, it also creates function as a ripe and readily available attack surface, introducing exponentially greater risks than the already onerous cyber impacts of data compromise or network failures.

Pragmatically, IT/OT convergence forces the legal profession to think in a new way about guiding clients, litigating liability and legislating to address an unprecedented dimension of threat.

## New Attack Surface, New Crimes and Liabilities?

OT professionals must focus on functional operation uptime for the infrastructure that drives our industrial economy. OT itself often leverages supervisory control and data acquisition (SCADA) systems. These SCADA systems allow industrial organizations to control a complex variety of industrial processes locally or remotely. IT enhances the OT capacity to monitor, gather and process real-time data regarding those industrial processes taking place, for example, on oil rigs, in turbines, water management systems, energy plants or manufacturing lines. This convergence allows data to be useful to its full potential; however, it must be put into a context that supports effective business and operational decision-making.

Take utilization improvement as an example. Consider an IT application on a piece of mechanical technology in a nuclear plant that can provide indicators of dangerous overheating points requiring a temporary shutdown of the equipment. If the machine operator can know these risks in advance, he or she can schedule the downtime to have minimal productivity impact on operation. That connected insight allows the plant to achieve greater functional utilization. It even potentially decreases maintenance costs.

But adding that IT layer onto the OT system also introduces cyber risk. What was previously separated is now integrated. Thus it requires a highly resilient and comprehensive security architecture that includes physical security, logical operational security *and* information security.

Consider a chemical plant, where chemical mixing is controlled by an IT overlay on a specific operational process. Without disabling a thing, a cyber-actor could deliver a devastating functional attack—a subtle change to chemical configurations which manifest long after the end product is in the market—leaving the chemical company exposed to liability suits and potential regulatory action.

This evokes some challenging questions. What law exists to pursue appropriate criminal penalties, or award civil damages to the individuals or entities harmed? Perhaps we need to revisit the way in which we think about the punitive ramifications of this kind of functional impact. First, who would have standing to raise a claim? What if the attack originated in another jurisdiction, such as an adversarial nation? What, if any, role does a nation state play when its citizens or enterprises are attacked?

This new reality may require changes in legislation. It also causes the United States to revisit how we advise clients on policies to protect against functional impact, on governance and on expanded liabilities that Board members and senior leadership may face in this converged environment.

## Competitive Tactics

The new threats arising from IT/OT convergence also raise the specter of a new age of competition. Acquiring a target technology or business that a competitor wants, even if the acquirer won't use it, is an often legal competitive practice. Denying the competitor access could weaken their brand position or expansion opportunities. But what about using a cyberattack to subtly manipulate a competitor's production quality to harm their brand longer term? How is that damage quantified? How is such a tactic punished? More importantly, what is the foundational level of security hygiene in a converged IT/OT environment that forms a new *de facto* standard of care? Must business attorneys now advise on the realities of the inevitable claims of negligence if such a security standard is not maintained?

As business advisors, attorneys practicing in our digital culture may have a responsibility to advise clients to prepare for such scenarios. While solutions to prevent these kinds of intrusions exist, implementing them in the correct way demands collaboration with IT security and operational experts. Clients should undertake a risk-based approach to limit liability while reaping the productivity gains of convergence.

## Impacts for Insurers

Finally there is the issue of insurance. We are seeing an increase in claims and litigation against cyber policies due to lost data as well as the operational losses arising from breaches. This could include down-time, data regeneration, customer notifications etc. In the converged environment, we may need to rethink the approach to insurance and not segregate cyber from other business operations coverage. After all, the impact of tainted products put into a marketplace from an "attacked" manufacturing line can include recalls, repairs, replacement and substantial valuation reduction. It is feasible that the insurance industry itself may begin requiring operational security and segmentation that exceeds the cyber hygiene requirements of an IT-only environment.

## Remedies

There are efforts under way to define guidance and standards that will help navigate the unique security landscape of converged IT/OT operations. Attorneys working in this sector will be well served to familiarize themselves with these new guidelines.

The U.S. Department of Homeland Security has recently established the Cybersecurity and Infrastructure Security Agency (CISA) under the authority of Public Law No: 113-278, Nov. 16, 2018, the "Cybersecurity and Infrastructure Security Act of 2018."

The very name implies the connectedness of IT and OT. As part of its efforts, CISA launched the Information and Communications Technology (ICT) Supply Chain Risk Management Task Force (the Task Force). The Task Force is a public-private effort with a unique focus. It seeks to assess cybersecurity risks and develop consensus

recommendations to manage risk to the global ICT supply chain. Task Force members include companies across the IT and communications sectors, together with government stakeholders from defense and civilian agencies. I have the honor of serving as a member of the Task Force Executive Committee.

As a first step, the Task Force plans to generate an inventory of U.S. federal and private sector supply chain risk management activities, best practices, and guidance to inform its work. Additionally, after evaluating multiple areas for optimum impact, the Task Force has established four working groups to:

- Develop a common framework for the bi-directional sharing of supply chain risk information between government and industry.
- Identify processes and criteria for threat-based evaluation of ICT supplies, products, and services.
- Identify market segment(s) and evaluation criteria for Qualified Bidder and Manufacturer List(s).
- Produce policy recommendations to incentivize the purchase of ICT from original manufacturers or authorized resellers.

This represents a unique collaboration on a comprehensive approach. The outcome of these workgroups may inform attorneys advising clients that provide ICT solutions to the U.S. government, and also serve as roadmap for a de facto standard of care for an IT/OT converged environment.

In addition, the U.S. National Institute for Standards and Technology (NIST) released draft Interagency Report 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks.* This offers guidance on a key area of vulnerability in the converged environment—the Industrial Internet of Things. The report provides guidelines to help organizations better understand and mitigate security and data privacy risks stemming from the proliferation of connected technologies that is occurring in traditional OT environments. Informed legal guidance will be particularly necessary here. This report lays the groundwork for new potential certification schemes or U.S. legislation to mandate basic cyber hygiene requirements, the violation of which could have far-reaching implications, much like the European Union Cybersecurity Law.

Interestingly, the European Cybersecurity Act creates a framework for certification valid across the EU. The certification would apply to products, processes and services. The Act further takes up the challenge of enhancing the security of connected products, IoT devices and critical infrastructure via such certification. For attorneys with multinational clients, monitoring and understanding the types of certification schemes being evaluated currently by the European Union Agency for Network and Information Security under the Cybersecurity Act is also recommended.

# Our Mandate

The profound changes deriving from IT/OT convergence require us to take a fresh look at legal and regulatory norms that have stood for decades since the Industrial Era. We are in a radical new environment where exponential benefits and risks are now reality. Clients, regulators and governments will rely on the legal community for informed insights and expanded guidance on a breadth of unprecedented issues and liabilities. We must be ready for this challenge.

**Edna Conway** *is Chief Security Officer, Global Value Chain, at Cisco.*