



The pointlessness of pointing fingers: Can business, IT, and OT stakeholders play nice?

To get to cyber resilience, organizations must develop a security governance framework that permeates the enterprise – from the boardroom to the shop floor.

Things are changing pretty radically in the energy, resources, and industrial (ER&I) space. Industry 4.0 and the emergence of autonomous systems powered by data, analytics, and AI are driving an unprecedented wave of transformation. A growing number of mergers, acquisitions, and divestitures are shining a light on systemic gaps, as are a rising number of cyber incidents and more rigorous board focus on cyber maturity.

The imperative to find innovative solutions to address endemic challenges—ranging from improved environmental performance to more collaborative community relationships—is altering operational realities. And the spread of COVID-19 has only accelerated this trend, forcing organizations to transition to remote work at breakneck speeds.

It's progressive. It's disruptive. And it's sparking conflict between the digital teams championing these new initiatives and the operational technology (OT) teams expected to operationalize them.

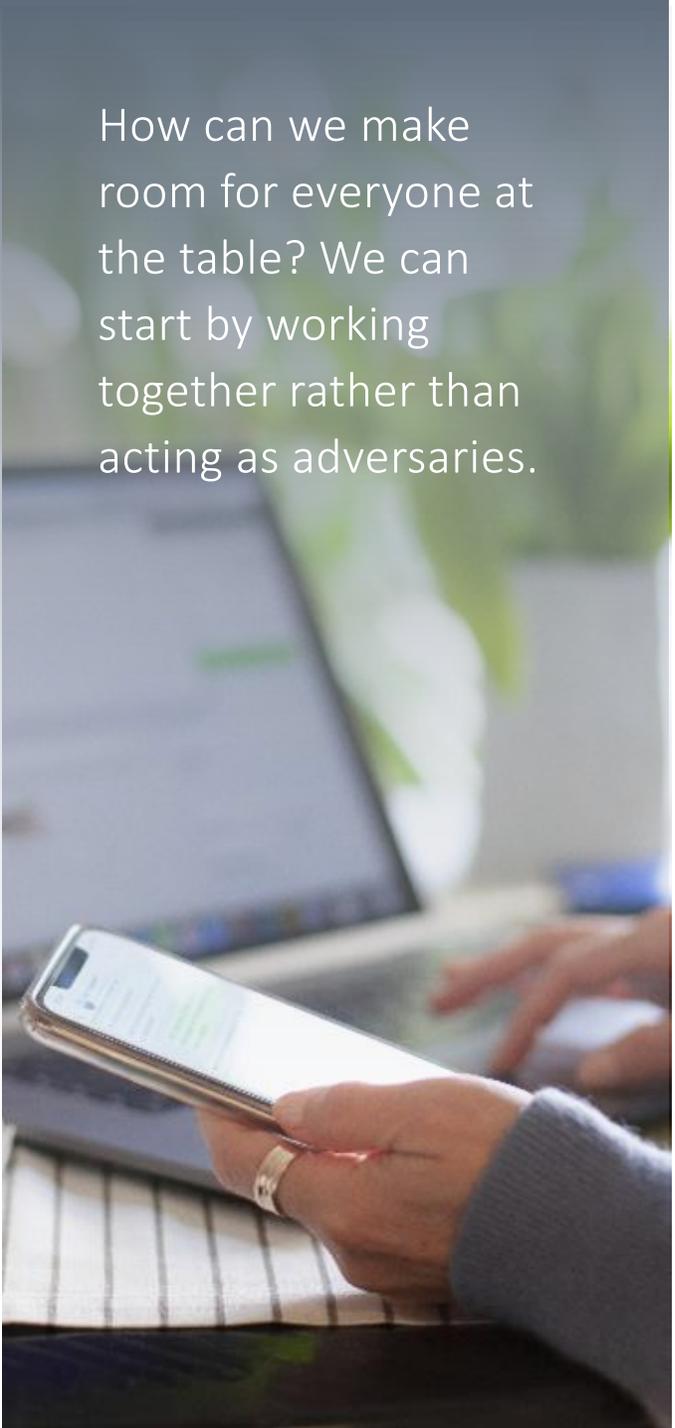
Cultural clashes between business, IT, and OT may not be new, but their fallout now threatens to take a toll that extends far beyond productivity challenges. They are also opening enterprises up to higher levels of cyber risk.

Sharing the risk

Missteps are happening at both ends of the spectrum. On the one hand, digital transformation teams tend to work in a rarefied environment that celebrates big ideas—even when those ideas veer from traditional operational practices.

Eager for the first-mover advantage, these teams sometimes fail to bake security into their processes from the outset, resulting in security lapses that unintentionally expose their organizations to a higher risk of breach. It doesn't help that many IT organizations are scrambling to keep pace with the risks introduced by digital initiatives, leading to potentially severe security control gaps.





How can we make room for everyone at the table? We can start by working together rather than acting as adversaries.

Cybersecurity at all levels

On the other hand, OT teams may be underestimating their vulnerability to cyberattack. Habituated to work in isolated factories and manufacturing environments, they often struggle to grasp how increased connectivity has changed the game.

Cloud computing, remote work, and extended supply chains have broken through the fortifications that once kept OT systems protected—presenting cybercriminals with a larger attack surface. In recent years, hackers have targeted supervisory control and data acquisition systems, programmable logic controllers, safety systems, and industrial control systems around the world.

According to a 2019 study conducted by Deloitte and the Manufacturers Alliance for Productivity and Innovation, 40 percent of respondents indicated their operations were affected by a cyber incident in the past 12 months, with attacks on manufacturing operations estimated to cost companies in excess of \$150 million. In one case, an attack on safety systems even put humans at risk. The ER&I sector is particularly at risk from these types of targeted attacks on power plants, autonomous vehicles, and remote operating centers.

These missteps are not going unnoticed. Every high-profile breach that hits the news creates greater reputational risk for a sector that is often assailed by negative publicity. In response, boards are placing mounting pressure on both business and OT teams to strengthen their cybersecurity postures.

Where to from here?

This is not simply about IT/OT integration or creating alignment between traditionally-siloed functions. To get to cyber resilience, organizations must dig deeper. This means developing a security governance framework that permeates the enterprise—from the boardroom to the shop floor.

Despite forming the backbone of digital transformation initiatives, cybersecurity still often falls under the sole domain of the IT function. This has to change. Instead, organizations must be able to create defined cybersecurity processes at the enterprise, business unit, and equipment levels. Similarly, they must clarify accountabilities at every level of the organization so that best practices can be embedded into people's daily work lives.

How can we make room for everyone at the table? We can start by working together rather

than acting as adversaries. Perhaps this means running war games or cyber simulations that encourage disparate teams to collectively respond to a hypothetical breach scenario. Perhaps it means creating a digital twin of your manufacturing facility as a playground for cross-functional stakeholders to stress-test your cyber resiliency and model out alternate scenarios.

These types of exercises aren't just about healing cultural rifts. They're about strengthening your cybersecurity posture so that when you face an attack (and you will), you have the functional maturity to effectively respond.

Contacts



Amir Belkhelladi | Canada Cyber Leader

abelkhelladi@deloitte.ca



Rene Waslo | Global Cyber ER&I Leader

rwaslo@deloitte.com



Ramsey Hajj | Global Cyber OT/ICS Leader

rhajj@deloitte.com



Dana Spataru | North South Europe Emerging Technologies Leader

dspataru@Deloitte.nl



Matthew William Holt | Global Cyber Emerging Technologies Leader

maholt@Deloitte.it

About Deloitte

Deloitte provides audit and assurance, consulting, financial advisory, risk advisory, tax, and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and service to address clients' most complex business challenges. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Our global Purpose is making an impact that matters. At Deloitte Canada, that translates into building a better future by accelerating and expanding access to knowledge. We believe we can achieve this Purpose by living our shared values to lead the way, serve with integrity, take care of each other, foster inclusion, and collaborate for measurable impact.

To learn more about Deloitte's approximately 330,000 professionals, over 11,000 of whom are part of the Canadian firm, please connect with us on [LinkedIn](#), [Twitter](#), [Instagram](#), or [Facebook](#).