MILE

Intelligence Desk

Special Edition

Welcome to this special edition of the MILE Intelligence Desk. In this issue, we sit down with Brian Finch, Public Policy Partner at Pillsbury, whose extensive experience in regulatory and government affairs advocacy has made him a recognized authority on global security and cybersecurity threats.

Brian provides legal counsel to companies across industries on regulatory compliance, cyber risks, national defense policies, and homeland security.

In our conversation, we explored the evolving cybersecurity regulatory landscape, the challenges foreign startups face when entering the U.S. market, and the critical role of trust and strategic partnerships in securing opportunities.



Brian Finch
Partner at Pillsbury Winthrop Shaw Pittman LLP

pillsbury

Brian is a Public Policy partner at Pillsbury with extensive experience in regulatory and government affairs advocacy. A recognized authority on global security and cybersecurity threats, he provides strategic legal counsel to companies across industries on regulatory issues, cyberattacks, national defense policies, and homeland security. He advises on risk mitigation, crisis response, and litigation strategies to minimize post-event consequences.

Regulation vs. Reality: Finding the Balance

MORIELLE LOTAN: You've advised U.S. utilities and private sector clients on cybersecurity investment while navigating regulatory complexities. How do you balance strong security measures with avoiding overregulation that may not yield meaningful improvements?

BRIAN FINCH: Over the past few years, we've seen a stark shift in cybersecurity regulation in the U.S. The previous administration leaned heavily on prescriptive regulations, often dictating security measures with little flexibility for companies.

This approach intensified after high-profile cyber incidents like the Colonial Pipeline attack, leading to rapid and costly mandates, such as the TSA Security Directive for pipelines.

In contrast, the current administration has adopted a more industry-driven approach, believing that companies understand their own risks best. While this allows for more innovative solutions, it also places greater responsibility on companies to justify their cybersecurity posture—especially as public companies must disclose their cyber risks and mitigation strategies.

Ultimately, the challenge is ensuring that regulation enhances security without being overly burdensome or disconnected from operational realities.

Cybersecurity & Energy: A New Market for Defense-Grade Solutions

MORIELLE LOTAN: With the U.S. Department of Defense (DoD) increasingly focused on energy security, what are the biggest challenges for Israeli and other foreign cybersecurity companies trying to secure U.S. contracts?

BRIAN FINCH: There’s no doubt that Israeli cybersecurity expertise is highly respected—especially in the private sector. The challenge in the U.S. defense and intelligence community is that there are mixed views on foreign cybersecurity products, including Israeli solutions. Some decision-makers approach them with skepticism, despite their proven track record.

That said, these challenges can be overcome by ensuring:

- Clear alignment with U.S. cybersecurity compliance frameworks (e.g., CMMC for defense contractors).
- Strong partnerships with established U.S. firms to ease procurement concerns.
- A direct focus on solving real operational pain points, rather than just offering theoretical or future-oriented solutions.

The key is speaking the language of U.S. buyers—whether in the energy, defense, or utility sectors—and demonstrating that your product isn’t just cutting-edge, but also seamlessly integrates into existing security requirements.

Trust & Market Entry: The Role of U.S. Presence and Strategic Partnerships

MORIELLE LOTAN: We often talk about how trust and boots-on-the-ground relationships are critical in the U.S. market. What are the best practices for foreign companies navigating this landscape?

BRIAN FINCH: Trust is everything. In the U.S. energy sector—whether it's electricity, gas, oil, or nuclear—companies and regulators want direct relationships with the people behind the technology. That means having a U.S. presence with American employees who can build credibility, respond quickly, and engage decision-makers directly.

Here's what works:

- **Local Expertise:** Companies that have American team members or dual citizens (e.g., U.S.-Israeli executives) find it easier to navigate contracts and compliance.
- **Industry Networks:** Getting involved with key trade associations and their cybersecurity working groups is invaluable. These groups help establish credibility and facilitate introductions to decision-makers.
- **Strategic Partnerships:** Working with established U.S. firms—either through joint ventures or as subcontractors—can significantly lower barriers to entry.

At the end of the day, successful market entry isn't just about having the right product—it's about being known, trusted, and embedded in the right networks.

What's Next?

Brian's insights underscore a critical shift in cybersecurity strategy—from prescriptive government mandates to industry-driven solutions. This shift creates opportunities for innovative security providers, but also raises the stakes for companies to proactively address cyber risks before regulations force their hand.



- The MILE Team