Proactive Framework Builds Assurance for Uncertain Times

kslawemail.com/71/6014/pages/page-15-new-harmon.asp

Zack Harmon and Dan Coats Return to King & Spalding to Launch National Security and Corporate Espionage Practice

In fall 2019 — within a month of each other — Zack Harmon and Dan Coats returned to King & Spalding after high-profile stints with the U.S. federal government, Zack as chief of staff to FBI Director Chris Wray and Dan as the director of National Intelligence.

For Harmon, who has also held leadership roles at the Department of Justice, returning to K&S made sense for several reasons. “The firm offered easily the best platform for the practice I want to build,” he said. “Working through our established government investigations brand will allow me to quickly rebuild (and expand) my investigations practice and leverage my recent experience, which includes just about every kind of investigation conducted by the federal government.”

For Dan Coats, whose distinguished career in public service includes serving as U.S. ambassador to Germany and as a U.S. senator and U.S. representative for Indiana, the firm’s platform also was a motivation: “The opportunity to reconnect with peers in other practices and across industries made returning to King & Spalding an easy decision.”

Both return to do more than rebuild their practices, however. They are also launching the firm’s National Security and Corporate Espionage (NSCE) Practice to advise clients about the rapidly evolving national security landscape and its immediate implications for their businesses.

Paradigm Shift: National Security Now Tied to Market Share

Today’s world economy offers great opportunity for global players, but that opportunity comes with a serious risk of theft of intellectual property, data and technology. In addition, the transactions landscape has become more complex, and timelines are less clear than ever.

Explaining the seed idea that led to the NSCE group's formation, Harmon indicated that there have been a number of significant paradigm shifts in the way governments around the world see national security. "Governments — including the U.S. government — now view national security as fundamentally tied to economic advantage, or in the simplest terms, market share."

Harmon's recent government work, along with the work of Coats and former senior counselor to the FBI director, Sumon Dantiki, focused on national security issues within the U.S. intelligence community. Harmon noted that on the national security side, K&S already has excellent data security, breach response and Committee on Foreign Investment in the United States (CFIUS) practices, "all of which are essential to the first-of-its-kind national security and corporate espionage practice we are building."

According to Harmon, among governments across the world, "it's now a widely held view that one key to national security is control of significant market share in important industries." This means that for many countries, it's become stated policy to aggressively pursue every possible angle to ensure business success for companies in their own country.

It's common knowledge that government players are stealing intellectual property, data and technology from industry leaders in other countries. But even beyond theft, these governments will use every tool they have to gain national advantage, whether it's how they structure research agreements or creating huge incentives to lure key people to work in their country. They are also using traditional espionage tactics as well as nontraditional means to collect information of all kinds.

Now more than ever, these players deploy powerful cyber tools to gain access to critical assets for commercial success: product formulations, customer databases and analytical tools for tracking market trends. As Harmon says, "If it's an asset that makes company XYZ successful, and if it's in a critical industry, there are governments around the world on a mission to capture those assets so companies in their own countries can use them to compete."

The New Competitive Threat: Sophisticated, Aggressive Nation-States

As a direct result of this paradigm shift, Harmon says that U.S. companies and academic institutions need to change the way they think about national security issues, because those issues have direct implications for their business operations.

"Companies have always understood that their competitors want their secret sauce. People running these companies have made judgments over the years about what their competitors are willing and able to do to put their hands on that secret sauce." The new threat — what they haven't been thinking about until recently — is that it's not just their competitors coming after them. There are now sophisticated, aggressive nation-states in

pursuit. It's now critical for these organizations to understand the growing scope of actual threats —what has happened in the past, and what tactics are in play now — so that they can be proactive and thorough about protecting their assets.

Navigating a Dynamic Regulatory Landscape

In addition to security standards, companies face a complex landscape of changing regulatory and procurement requirements. It's key, therefore, to stay abreast of this evolving landscape.

All of these changes — for example, the build-out of CFIUS under the new Foreign Investment Risk Review Modernization Act (FIRRMA) legislation and heightened cybersecurity requirements for companies to follow — create a substantial burden for companies engaged in global commerce. According to Harmon, "All this happens because our government is increasingly concerned — and rightfully so — that key assets within U.S. companies are evaporating out the back door. So the government increasingly involves itself to make sure U.S. companies are protecting themselves."

But there's a limit to just how much protection the government can ensure through regulation and legislation. So forward-thinking companies are viewing operations through this new national security lens and taking steps to reconsider how they operate.

As Harmon points out, "You don't need to be an artificial intelligence company to be using and developing key AI technologies. You could be a manufacturer or a logistics service provider. Companies all over the map in every industry are developing technologies that are innovative and very helpful — and these technologies can be applied in any number of ways by governments and competitors overseas."

Transactions Get Stickier — and Take Longer to Close

As the U.S. government imposes increasingly stringent regulations and disclosures around transactions, it's now much harder than it used to be to navigate transactional processes. CFIUS is a prominent example: now when a U.S.-based company seeks direct or indirect investment by a foreign government, the CFIUS process applies.

A CFIUS review can take a significant amount of time. From a transactional standpoint, elapsed time matters to companies. They need to know how long they are going to be held up in this process, and they want to know whether there's a chance the U.S. government may ultimately tell them they can't do the deal.

"With executive branch agencies and Congress showing increased interest in transactions, questions abound: agencies could reach out, Congress could reach out, any of which could hold up a deal," Harmon said. "If you're in the deal business, this uncertainty is an issue."

“We counsel clients for all of these issues,” Harmon continues. “We help a business fundamentally understand what assets are at risk and how to protect those assets better. Further, we can outline key steps to mitigate the risks associated with a security breach and, when there’s an incident, counsel clients how to mitigate the legal risks that follow in its wake.”

Harmon concludes, “In today’s world, it’s incumbent upon a business to prepare for all the regulatory and legal risks associated with a security incident. I came back to the firm because of our capabilities to do just that, at the highest level.”