RANE Risk Assistance Network + Exchange

RANE Event Recap | April 10, 2018

2018 RANE Risk Management Roundtable on Economic Espionage: Protecting Corporate Assets and Shareholder Value

FEATURED EXPERTS

Luke Dembosky, Co-Chair, Cybersecurity and Data Privacy Practice, Debevoise & Plimpton LLP

Kevin Hayes, Senior Principal, Promontory

David J. Hickton, Founding Director, University of Pittsburgh Institute for Cyber Law, Policy, and Security

David Lawrence, Founder and Chief Collaborative Officer, RANE

Bill Priestap, Head of the Counterintelligence Division, Federal Bureau of Investigation (FBI)

Adam Segal, Ira A. Lipman Chair in Emerging Technologies and National Security, Director of the Digital and Cyberspace Policy Program, Council on Foreign Relations (CFR)

Rhea Siers, Executive Director, Cyber & Information, RANE

Elad Yoran, Executive Chairman, KoolSpan and CEO, Security Growth Partners (SGP)

In Partnership with

Debevoise & Plimpton

From state actors to corporate insiders, company secrets are at risk from a number of threats and on a number of fronts, including traditional covert actions as well as newer cyber attacks. In addition to the financial, operational, and reputational risk to the company, these actions can also pose a threat to U.S. economic and national security.

Amid this growing threat, the 2018 RANE/Debevoise & Plimpton Risk Management Roundtable recently brought together a wide array of corporate executives, leading experts, regulators, and lawyers to examine the economic espionage landscape and offer insights on what companies can do to be better prepared to protect their valuable IP.

The highlights from the roundtable's two keynote interviews and panel follow.

THE STATE OF ECONOMIC COMPETITION AND IP THEFT BETWEEN THE U.S. AND CHINA

- To begin to dissect the issues surrounding economic espionage, the first keynote interview of the day, with **Adam Segal** of the Council on Foreign Relations, focused on how and to what degree U.S. firms can mitigate the risk of losing trade secrets and valuable IP when doing business in major emerging economies such as China and India. "***U.S. companies have to figure out if they are going to engage in those markets, what they are willing to***

part with," he told **David Lawrence** of RANE. Japanese companies like Toyota, **Segal** said, have been much more careful about what they transfer when doing business in China, for instance. "You look at what Toyota and the other manufacturers were transferring, especially when it came to their vehicles, which they knew the Chinese were going to be interested in. They never moved the battery and the engine, but everything else was made in China, then put in a black box."

- ***American companies are starting to take a similar, more carefully calibrated approach***, according to **Segal**. Very often that means they will only conduct ***sensitive operations or product development at the very beginning or at the very end of their R&D cycle***. "If [local] employees in these countries walk out with secrets at either end of the cycles, the damage is not as great," **Segal** noted.

- Until recently, U.S. and European companies entering risky but lucrative markets like China were willing to accept that losing some of their IP in the process was the necessary cost of doing business there. Central to that calculation, **Segal** explained, was the ***confidence that they could continue to innovate faster than the local enterprises and always stay one step ahead from a competitive standpoint***. But that same confidence isn't so evident any longer, and for good reason. "Previously it was easy to write off these countries as simply rising science and technology powers, we knew they were spending more but the U.S. competition and innovative capabilities seemed head and shoulders above the rest. ***Now there is a real worry about the competitiveness of others. China, for instance, is spending more than the U.S. is***," **Segal** noted. Chinese spending on R&D and basic science, for instance, have increased double digit for almost 20 years while the U.S. has been flat for at least 10 years, he pointed out. "We had the same worry with the Japanese. But the Japanese, despite the economic tensions, were allies. The Chinese are not allies, and the Russians certainly are not allies so the worry is broader."

- The competition for economic knowledge and expertise is only going to significantly increase between these powers, and the U.S. and Europe. "Competition is getting worse. We don't have too many constraints right now on geo-economic relations and the great power rivalries," **Segal** said. Relations between Russia and the West are rapidly deteriorating in the wake of the poisoning of a former Russian spy and his daughter in the UK, with tit-for-tat diplomatic expulsions only further fraying ties that have already been damaged by sanctions in recent years. Even more importantly, **Segal** cautioned, ***U.S./China relations are going to get much worse*** now that the Trump Administration has invoked Section 301 of the Trade Act of 1974 to impose new tariffs against China, take its case to the World Trade Organization court alleging theft from and coercion of U.S. companies doing business in China and block a lot of Chinese investment in the U.S. "The U.S. is going to look for ways to retaliate for all of this intellectual property that has left the country. When this happens, the Chinese will, in turn, also look for retaliation. These trends are negative, and I suspect that the competition over technology is just going to get worse and that U.S. companies are going to get squeezed," **Segal** said.

- On top of this, there might also be an ***unraveling of the U.S.-China cyber agreement***, **Segal** said. In 2015, China's President Xi and President Obama signed an agreement that said neither side would knowingly support nor tolerate cyber-enabled theft. After the agreement was signed, the publicly available data seemed to show a decline in these incidents. However, there seems to have been a slight uptick recently where the Chinese are exploring the grey zone, are going after dual use technology, or are beginning to ignore the agreement altogether.

Bill Priestap of the FBI warned that too many US companies and executives still think economic espionage is limited to aerospace, defense or technology sectors. "My message today is if a U.S. company is a world leader in an industry, it is likely being targeted by a foreign adversary."

THE FBI AND COUNTERING THE ESPIONAGE THREAT

- The second keynote interview of the day, with **Bill Priestap** of the FBI, looked at the role of the Bureau in helping companies combat economic espionage. "The FBI is trying to protect America's vital assets. That includes everything from state secrets to trade secrets, because we are seeing ***a severity of the threat in the counter-intelligence realm that, in my career, we've never seen before***," **Priestap** declared at the outset. The bottom-line, he continued, is that the traditional ways of approaching the problem — collecting intelligence, investigating wrongdoing, prosecuting wrongdoers with the Department of Justice, and penalizing the wrongdoers — is not sufficient to match the severity of today's threat. "When we talk about the Bureau protecting America's vital assets, those vital assets most of the time are not the U.S. government's, but the private sector's. So what the FBI is trying to do more than in the past, is try to get the word out so that we can help the private sector better protect its assets," **Priestap** stated. "Our workload in economic espionage continues to grow, and the more we look, the more we're finding, unfortunately."

- **Priestap** counseled that companies have to take a more expansive view of economic espionage, because too many firms and executives still think that it is limited to aerospace, defense or technology sectors. "My message today is ***if a U.S. company is a world leader in an industry, it is likely being targeted by a foreign adversary***.

- A case that proves this point, showing how state actors like China will use unexpected methods to go after non-traditional targets, is what the FBI has called the "***corn seed case***", which involved DuPont Pioneer, an agro-science giant that was trying to develop more productive corn seeds. One day, an employee at DuPont saw an individual digging in the company's fields and literally pulling up seeds. "***What we learned after a two-year investigation was that there was an entire network of individuals based in China that were trying to steal experimental corn seeds not just from DuPont Pioneer in Iowa, but also in Indiana and Illinois***," **Priestap** said. The U.S. is the largest exporter of corn in the world and its biggest customer is China, which had determined that it wants to be more self-sufficient, not just in agriculture but in a number of other fields. "The bottom line is this network of state actors were trying to steal U.S. corn seeds so that they could grow more corn in China and import less corn from the U.S." **Priestap** explained.

- Given the preponderance of insider threats, **Priestap** also advised companies to be ***very careful about their hiring processes***. "The importance of due diligence before making hires cannot be overstated. Once these employees are on board, companies have different policies as far as being aware of their employees' activities, but to give them carte blanche just because they are already an employee can be very dangerous," he said.

THE KEYS TO A CORPORATE COUNTER-INTELLIGENCE PROGRAM

- Near the end of his interview, **Bill Priestap** stressed that acknowledging the severity of the threat to Western businesses is the first step in helping to stop it. And indeed, during the day's panel discussion, a number of experts stressed that ***a lack of awareness is still a major obstacle***. "Financial institutions tend to be focused on fraud," said **Kevin Hayes** of Promontory. "Although they are increasingly focused on cybersecurity generally, there is still a lack of awareness in terms of the threat from foreign intelligence organizations. Financial institutions are more and more focused on the organized crime threat, but the connectivity of that, to the threat from foreign intelligence has only just started." Financial firms also tend to be more concerned with

"It's important to lock [new] employees in to knowledge of the company's policies and procedures regarding what they can and cannot do with company data," said Luke Dembosky. "It's also essential that the company actually follow its written policies and procedures…because the lack of adherence to one's own standards becomes a liability in a trial or regulatory proceeding involving a data incident."

protecting their customers' Personally Identifiable Information (PII), since many of them have run into trouble with regulators because of mishandling. And many in the industry still have the misperception that they are not prime targets because they are not necessarily developing the type of advanced IP that would be of interest to foreign adversaries.

- **Elad Yoran** of Security Growth Partners echoed Hayes' points, stressing that companies need a ***more well-rounded perspective that not only focuses on China and traditionally vulnerable industries such as defense, aerospace, and cyber***. He said that although awareness about the threat is very high internationally, inside the U.S. it's still "embarrassingly low." **Yoran** recounted a conversation he had had with a Chief Security Officer (CSO) of a global, midsized financial services firm headquartered in the U.S. "We talked about the threat of international corporate espionage and I asked how he was addressing it. He said that it was not in his top five, which meant he was not going to do anything about it from a technology point of view."

- For **Yoran**, the lack of awareness today extends to where he believes the real battle is — the devices that we use to talk, text, and conduct an increasing amount of our virtual lives, both at work and home. "We have a very good handle on the more general network and broader IT. ***Where we are woefully behind is in the mobile device and, in particular, on the mobile communications side of things***. I believe that the easy, inexpensive and effective solution to these is the use of end-to-end encryption (E2E), whether it's a phone call or other data."

- As **Bill Priestap** of the FBI had mentioned, thoroughly vetting employees is a critical part of reducing the threat of economic espionage. **Luke Dembosky** of Debevoise & Plimpton said one sometimes-overlooked step in the hiring process is ***how companies go through the paper work involved in onboarding and exiting employees***. "It's important to lock employees in to knowledge of the company's policies and procedures regarding what they can access and what they can and cannot do with company data. It's also essential that the company actually follow its written policies and procedures. It is almost worse to write ones that that the company does not follow because the lack of adherence to one's own standards becomes a liability in a trial or regulatory proceeding involving a data incident and certainly makes them difficult to enforce against employees," **Dembosky** said.

- ***Building a counter-intelligence program is not about veering away from the basics of due diligence***. "I don't look at stopping industrial espionage, foreign adversaries, and IP theft as being any different from preventing the type of things that companies would be focused on anyway such as PII and monetary loss. It is the same type of technical controls," **Hayes** said. "If you can enforce strong technical controls, you would go a long way toward managing the insider threat as well as countering external intruders."

- However, **Hayes** does not think that the technical controls are the most important tools. He pointed to research on a thousand actual insider threat events that showed the ***majority of those incidents were detected by audit, customer complaints, and co-worker suspicion instead of technical controls***. **Rhea Siers** of RANE agreed that technical tools are useful, but companies should not be over reliant on them. "What you are trying to create here is the ***equivalent of a human firewall***, even if firewalls are no longer as popular in the cyber business," she said. Firms must also make sure that the tech tools they are using are not so jargon-packed that everyday users cannot understand what they should be gleaning from them.

Very often US companies in markets like China will only conduct sensitive operations or product development at the very beginning or at the very end of their R&D cycle. "If [local] employees walk out with secrets at either end of the cycles, the damage is not as great," Adam Segal noted.

- ***Knowing what you are protecting*** is also key to building an effective counter-intelligence program. "Firms have to be incisive about what you're protecting. They cannot protect everything since it is way too expensive," said **Siers**. "There is an awful lot of preparation that needs to occur aside from those for the crown jewels. People need to be convinced that this is not just about someone getting the formula for Coca-Cola. The team in charge of counter-intelligence also has to work in advance to figure out what the company's Achilles heel is."

- "Companies also have to be somewhat cognizant of their threat vectors," which can include state actors and transnational criminals, **Siers** continued. Before an actual attack takes place, organizations need to decide what the ***threshold is to initiate a thorough investigation*** of a particular threat. For these programs to be effective, reporting mechanisms that go all the way to the top are needed.

- Part of knowing what to protect is ***getting sound advice***. "Dealing with a good law firm can represent you and put you in a good compliance program that could navigate, particularly for big multinational companies, the various chambers of reporting, which are different around the world," **David Hickton** of the University of Pittsburgh said. In terms of dealing with law enforcement, having good legal representation can help companies assert themselves and get the right briefings. Companies can also tap the ***National Cyber Investigative Joint Task Force*** where they can get ***valuable threat briefings*** while working directly with the IT department.

- Lastly, **Siers** cautioned that while companies do need to think carefully about how to set up such a program, taking too long is not an option. People who are seeking targets are actually looking for companies that react slowly. ***So if firms have vested their authority or program in a slow-moving part of the company, it has to reconsider***. The best model, she said, has to eliminate silos, for example those between physical security and cyber security teams, and the overall team leader should be someone in the C-Suite or the firm's General Counsel.

"Financial institutions tend to be focused on fraud," said Kevin Hayes. "Although they are increasingly focused on cybersecurity generally, there is still a lack of awareness in terms of the threat from foreign intelligence organizations."

ABOUT THE EXPERTS

Luke Dembosky, Co-Chair, Cybersecurity and Data Privacy Practice, Debevoise & Plimpton LLP
Luke Dembosky is a cybersecurity and litigation partner with Debevoise & Plimpton. His practice focuses on cybersecurity incident preparation and response, related civil litigation and regulatory defense, and national security issues. Dembosky joined the firm in 2016 after serving as Deputy Assistant Attorney General for National Security at the Justice Department, where he oversaw DOJ's first national security cyber portfolio. Over a distinguished 14-year career, he led the Department's work on many landmark cyber cases, including the Target, Sony Pictures, Home Depot, Anthem and OPM breaches.

Kevin Hayes, Senior Principal, Promontory
In his current position at Promontory, Kevin Hayes specializes in information security risk management and defense of networks and national critical assets from advanced foreign adversaries. He has worked extensively on cybersecurity enhancements, and privacy risk and control assessments of major U.S. financial institutions. Before joining Promontory, Hayes served in a diplomatic role at the British Embassy in Washington, and spent many years in a variety of UK government information-assurance and security roles at the Government Communications Headquarters.

David J. Hickton, Founding Director, University of Pittsburgh Institute for Cyber Law, Policy, and Security
Prior to his current position at the University of Pittsburgh, David J. Hickton served as United States Attorney for the Western District of Pennsylvania. Before that, he engaged in private practice, specializing in the areas of transportation, litigation, commercial and white-collar crime. For more than a decade, Hickton was an adjunct professor at the Duquesne University School of Law, where he taught antitrust.

David Lawrence, Founder and Chief Collaborative Officer, RANE
Before starting RANE, David Lawrence served for approximately 20 years as Associate General Counsel and Managing Director at Goldman Sachs. During his tenure, he formed and was the global head of the Business Intelligence Group, where his role covered a wide range of legal, regulatory, diligence and transactional responsibilities for the firm, as well as advising clients directly. Prior to joining Goldman, Lawrence served for 10 years as an Assistant US Attorney in the Southern District of New York, where he was the Deputy Chief of the Criminal Division and Chief of the Public Corruption and General Crimes Units.

Bill Priestap, Head of the Counterintelligence Division, Federal Bureau of Investigation (FBI)
Bill Priestap oversees all of the FBI's Counterintelligence investigations and operations and is responsible for ensuring the Bureau successfully executes its national security mission to defeat foreign intelligence threats and activities. Priestap most recently served as the Deputy Assistant Director (DAD) of the Intelligence Operations Branch, where he oversaw HUMINT operations, integration management, and strategic technology. Since he began his FBI career in 1998 working organized crime and drug matters in the Chicago field office, Priestap has served in a variety of counterterrorism, intelligence and counterintelligence roles at both the New York field office and FBIHQ in Washington.

Adam Segal, Ira A. Lipman Chair in Emerging Technologies and National Security, Director of the Digital and Cyberspace Policy Program, Council on Foreign Relations (CFR)
An expert on security issues, technology development, and Chinese domestic and foreign policy, Adam Segal was the project director for the CFR-sponsored Independent Task Force report "Defending an Open, Global, Secure, and Resilient Internet". Before coming to CFR, he was an arms control analyst for the China Project at the Union of Concerned Scientists. Segal has taught at Vassar College and Columbia University, and been a visiting scholar at Stanford, MIT, the Shanghai Academy of Social Sciences and Tsinghua University in Beijing. He is the author, most recently, of "The Hacked World Order: How Nations Fight, Trade, Maneuver and Manipulate in the Digital Age" (Public Affairs, 2016).

Rhea Siers, Executive Director, Cyber & Information, RANE
During her thirty years of service in the US Government, Rhea Siers dealt with some of the most critical issues facing the Intelligence Community including cyber operations, information sharing, counterterrorism and counterintelligence. She served as NSA's senior representative to the FBI, as well as NSA's Deputy Associate Director for Policy, led operational and intelligence production as a senior manager, and served in the NSA Office of General Counsel. As an attorney and policy expert in the cybersecurity arena, Siers has worked with companies and organizations designing cybersecurity programs that meet regulatory needs and are tailored to the challenges of different industries.

Elad Yoran, Executive Chairman, KoolSpan and CEO, Security Growth Partners (SGP)
Elad Yoran is a 20-plus year cybersecurity veteran, having founded, led and advised many foundational cyber start-up companies, including Riptech, MediaSentry, Sentrigo, Red Owl Analytics, and Threatgrid. He previously served as VP of Global Business Development at Symantec, and now serves as director at Infinidat as well as on several government and industry boards such as the Army Cyber Institute and the Cloud Security Alliance.

ABOUT DEBEVOISE & PLIMPTON, LLP

Debevoise & Plimpton LLP is a premier law firm with market-leading practices, a global perspective and strong New York roots. Our clients look to us to bring a distinctively high degree of quality, intensity and creativity to resolve legal challenges effectively and cost efficiently. Deep partner commitment, industry expertise and a strategic approach enable us to bring clear commercial judgment to every matter. Approximately 650 lawyers work in eight offices across three continents, within integrated global practices, serving clients around the world.

ABOUT RANE

RANE (Risk Assistance Network + Exchange) is an information and advisory services company that connects business leaders to critical risk insights and expertise, enabling risk and security professionals to more efficiently address their most pressing challenges and drive better risk management outcomes. RANE clients receive access to a global network of credentialed risk experts, curated network intelligence, risk news monitoring, in-house analysts and subject matter experts, and collaborative knowledge-sharing events.