2015

Profile in Public Integrity: Daniel E. Karson

Center for the Advancement of Public Integrity

CENTER FOR THE ADVANCEMENT OF PUBLIC INTEGRITY

COLUMBIA LAW SCHOOL
JEROME GREENE HALL
435 WEST 116TH STREET
NEW YORK, NEW YORK 10027
(212) 854-6186
WWW.LAW.COLUMBIA.EDU/CAPI

Profiles in Public Integrity: Daniel E. Karson

Daniel E. Karson is Chairman of Kroll, based in the New York office. Dan has more than 40 years' experience directing investigations of business crimes. His practice areas include major fraud investigations, the Foreign Corrupt Practices Act, litigation support, contests for corporate control, Internet crimes, financial crimes, asset searches, product counterfeiting and due diligence.

Dan launched Kroll's European operations, opening its London office and serving as its first Managing Director in 1986. Dan also opened Kroll offices in Boston and Philadelphia, and served as Kroll's General Counsel for eleven years.

Prior to joining Kroll, Dan was General Counsel and Assistant Commissioner of the Department of Investigation of the City of New York, where he conducted major fraud investigations. At DOI, he was also the First Director of New York City's Inspector General program and supervised the internal investigations offices of 24 mayoral agencies. Previously, Dan worked as an Assistant District Attorney of Bronx County, serving as Chief of Narcotics Investigations.

Before you joined Kroll, you spent time as an Assistant District Attorney and also working for the Department of Investigation, New York City's anti-corruption watchdog. How did these experiences inform your work at Kroll?

I was always interested in getting to the bottom of a corruption case – starting with an accusation by a whistleblower or working up the ladder of a criminal enterprise through informants. After nine years as a prosecutor I felt that my choices were to either make a career in government or to join a law firm or law department. Then I learned of Kroll, which at the time was a one-office firm building a reputation investigating business crimes. It seemed perfect fit for me and I never looked back.

You've been at Kroll for 30 years, during a time of enormous technological advances in all facets of society. How has the field of corporate investigation and intelligence changed over that time?

Technological advances have thrust upon us an age of information that was inconceivable even 30 years ago. Since Kroll is in the fact-finding business we have developed or acquired the latest information technology at each stage of its enhancement. We continue to add these tools to our investigative capability.

The other major change in our world comes, not surprisingly, in technology-based crimes. Thirty years ago employees were first starting to work on desktop computers, with no email or social networking. The fastest growing part of our business is the investigation of cybercrime: hacking and the theft of customer data, employee data, intellectual property and money. We have an international team of former FBI cybercrime agents and our own forensic laboratories worldwide. On the other hand, while the tech revolution has created a new type of crime and a new breed of criminal, old fashioned bribery and kickbacks are alive and well. Those are cases involving moneys paid to purchasing agents or foreign government officials. We are always investigating one of those cases at any given time.

You've said many times that Kroll is in the integrity business. What do you mean by that?

Our stock-in-trade is investigating the theft and loss of money, property, and private data, either through outright stealing or indirectly through bribery. In due diligence cases, we look for misstatements and omissions made by our clients' counterparties and verify the representations and warranties made to our clients in business transactions. Consequently, we are a resource for assuring honest dealing in business.

Many experts believe that the strategic and systematic use of big data is the future of anti-corruption enforcement in our cities. Do you agree? How can a company like Kroll help to make this future a reality?

I do agree. Data analytic tools enable swifter and more accurate fact finding, and we're only in the early stages of their application. For example, we know so much about how purchasing fraud is committed that we can program an accounts payable system to report data to us that will make corruption indicators jump off the spreadsheet – for example, by matching vendor addresses against employee addresses. You might think that a corrupt employee would not be so lazy as to use his or her own address as the location for a fictitious or self-dealing business, but it happens. At the government level, the use of analytics is even more important, because government accounting and purchasing systems tend to be more cumbersome, bureaucratic, and inefficient, if only due to their size and breadth. By successfully applying analytic tools we have used, governments can minimize or even eliminate purchasing fraud, ghost employees, false claims for disability, and similar examples of crime and waste.

As we all know, companies and governments alike face enormous and increasing threats of data breaches and other cybercrime episodes. Indeed, your colleague Alan Brill gave a fascinating, albeit frightening, presentation at CAPI's Global Cities conference this past spring about some of those risks and how they can be minimized. Are you finding that your clients are now up to speed on these issues, or do our governments and corporations still have a lot to learn to keep their systems, information, and money secure?

Crime walks in lockstep with technology, and every day we see examples of massive data breaches in the private and public sector. Many businesses and governments "get it," but enough don't that we'll continue to read about these disasters. Nothing is foolproof, but so much of prevention is in observing rules, such as:

- Change passwords frequently,
- Don't open emails from unknown parties,
- Never click on an attachment from an unconfirmed, unfamiliar source,
- Be suspicious of an email from a colleague bearing your company domain name but differing, however slightly, in format (XYZ.com vs. XYZdata.com), which may be a phishing attempt,
- Don't give email accounts or administrative passwords to vendors whose employees haven't been screened and whose IT systems' security hasn't been verified,
- Instruct employees to verbally confirm with people they know any unusual instructions, such as wire transfers to a new account for a regular vendor. That scam has cost businesses more than a half billion dollars in the last 2 years.

Just observing these policies can move a hacker on to the next target. The hard part is getting your employees to follow through. The hacker from China, Russia, Ukraine, or elsewhere is looking for the path of least resistance. It need not be your company.