Managing Risk

Raymond W. Kelly

An Interview with
Raymond W. Kelly, Vice Chairman, K2 Intelligence

EDITORS' NOTE *Ray Kelly is a distinguished leader and New York City's longest-serving police commissioner. He established the first Counterterrorism Bureau of any municipal police department in the country and built the Department's Intelligence Bureau, creating a global intelligence program with detectives stationed in cities abroad. The first Real Time Crime Center in America was also established by Kelly. He joins K2 Intelligence from Cushman & Wakefield, where he was President of the firm's Risk Management Services group. In the private sector he has also served as President of Investigative Group International and as Chief of Security at Bear Stearns. Kelly is a Distinguished Visiting Fellow at the Council on Foreign Relations and an ABC News consultant. His almost 50-year career in public service includes serving as commissioner of the U.S. Customs Service and as Undersecretary of Enforcement at the U.S. Treasury Department for which he received the Alexander Hamilton Medal. He served as a Vice President of Interpol and directed the International Police Force in Haiti, where he was awarded the exceptionally meritorious service commendation from the President of the United States. Kelly is also a retired United States Marine Corps Reserves colonel with 30 years of service in the United States Marine Corps Reserves, including serving a combat tour in Vietnam. He received 14 citations of merit for outstanding police work during his tenure at NYPD and was awarded France's highest decoration, the Legion d'Honneur. He is the author of the best-selling book* Vigilance: My Life Serving America and Protecting Its Empire City. *Kelly received his J.D. from St. John's University School of Law, his L.L.M. from New York University Graduate School of Law, his M.P.A. from the Kennedy School of Government at Harvard University, and his B.B.A. from Manhattan College. He is an attorney and a member of the New York State Bar.*

COMPANY BRIEF *K2 Intelligence (k2intelligence.com) is an industry-leading investigative, compliance and cyber defense services firm founded in 2009 by Jeremy M. Kroll and Jules B. Kroll, the originator of the modern corporate investigations industry. Over the past 40 years, Jules, Jeremy, and their teams have built a reputation not only for investigative, analytic, and advisory excellence but for the independence and insight they bring to investigations. With offices in New York, London, Madrid, Tel Aviv, Geneva, and Los Angeles, K2 Intelligence advises governments, companies, boards, and individuals in business areas including: Complex Investigations & Disputes; Anti-Money Laundering and Regulatory Compliance; Construction and Real Estate Project Oversight Monitoring & Compliance; Data Analytics & Visualization; and Cybersecurity Investigations & Defense.*

When the opportunity presented itself at K2, what made you feel it would be the right fit?

I had known of Jules Kroll (founder) for at least 40 years. He's an iconic figure in the business investigation and intelligence industry. He has, to this day, an ongoing reputation of very high standards for professionalism and integrity.

I was immediately attracted to this. I was aware that Jules had sold Kroll and started this operation with his son Jeremy, who I also knew. It seemed to me like the ideal combination.

There are a lot of smart young professionals here who possess quite an array of talents. We have many lawyers, skilled investigators, forensic accountants, and people with vast government experience – federal, state, and local.

One of the mantras here is that we use a multidisciplinary team and this is essential. The world is becoming more complex so if people are willing to pay us to solve issues, they need to be addressed in a multifaceted way.

Looking at the broad array of challenges and risks, are there specific areas that you focus on?

There is a lot of cross-pollination going on as far as commercial problems are concerned, but one of the enduring issues of our time is cyber intrusion. This permeates many areas that companies deal with today.

We're focused on risk management and addressing physical security issues but, even with that, there is often an element of cyber – it touches everyone's lives. These days, there is great risk of being hacked or intruded upon by professionals, foreign governments, or recreational hackers.

Ultimately, the biggest risk for most companies is financial. Hackers are primarily looking to steal money. We see the development of things such as ransomware, which is very difficult to mitigate depending on the systems that exist in a particular firm. Ransomware is where your data gets locked down, and it cannot be accessed unless you pay the ransom, usually in bitcoins.

If a firm has linked systems, the chances are that all of them are going to be impacted by these attacks. A way of avoiding this is to have networks that are totally independent from each other.

Ransomware is a threat that has been with us for years and it's nettlesome as there is no easy way to address it.

Every industry must be concerned because it exists across the board regardless of what business you're in.

How prepared are corporations today to fight the sophistication of these hackers?

The challenge is elevating awareness of the threat to the C-suite. The CEO, understandably, is focused primarily on making money. Some are resistant to spending money to prevent something that may never happen.

The Chief Information Officer is undoubtedly concerned about cyber threats but doesn't necessarily have regular access to the CEO or to board members.

Elevating awareness of the dangers of cyber intrusion to the highest levels of the company is an important goal.

Unless the CEO is involved, the implementation of a comprehensive and effective cyber program is probably not going to hold. There needs to be consistent attention from the top because the cyber threat is ongoing and must be continually monitored.

Is Chief Information Security Officer a role that every company needs to have filled today?

Financial institutions need to have a Chief Information Security Officer. Whether it's needed in other industries is a decision that individual companies must make depending on a variety of factors including size, vulnerability, and the type of business they're in. Ideally, I would like to see every company have someone in that role.

Is the K2 client the larger, more complex institution or is it much broader than that?

We have clients of all sizes. If we work with big companies, chances are they have a

robust internal capacity to protect themselves because they have the resources. We provide advice to them. The medium-size companies are less likely to have that. This is where much of our business comes from.

When services can sound similar across companies, does it come down to your people or the technology?

It ultimately comes down to people and the training they receive.

Some companies have a fairly comprehensive training program for new employees. I recommend that cyber defense and protocols be addressed before new employees ever touch a computer. About 80 percent of the intrusions we see come from employee carelessness.

Competency in cyber protection depends to a certain extent on the quality of people that are being hired. Ideally, they would all be people who have some experience or knowledge of the cyber threat.

Something as simple as clicking on an attachment can open the spigot and lead to the system becoming polluted. We can train people to be aware of that, but humans will make mistakes. These days, phishing attacks are quite sophisticated so employees have to be constantly aware.

Are the risks different today than they once were or are we just hearing about them more?

Cyber has changed the game. One of the other things we preach is that every company has to have a business continuity plan. It is a plan to get your company back in operation in the event of a catastrophic occurrence. In order to develop that plan, a company has to assess its key assets. These are the resources where, if they are lost, the company can't operate. Then we construct a detailed mitigation plan to address vulnerabilities.

A company needs to have a crisis response team that addresses these and other threats. The team must have enough authority to get things done.

We look at threats from natural disasters, terrorism, criminality, and cyber. The one that has grown in importance and criticality is cyber.

A company needs to have a crisis response team that addresses these and other threats. The team must have enough authority to get things done.

Does the understanding that this will affect the bottom line have to be there?

It does, but it often doesn't become an issue until it's too late. There are companies that have gone out of business as a result of a cyber-attack. We don't hear much about them because this is not something anyone wants to advertise.

On another issue, is it disheartening to see where the relationship between the police and the public has gone?

From my perspective, the relationship between the police and community is much better than it was 40 years ago.

We've had some problems, most of them a result of what appears in videos to be bad conduct on the part of the police.

I believe certain changes have to be made in policing, and some of them will take much longer than others. For instance, to regain trust, body cameras should be adopted by the police.

I believe we will see cameras becoming a part of police uniforms across the country in five to seven years. This will go a long way in regaining trust that may have been lost as a result of these jolting videos.

Also, I believe every police officer should have a four-year college degree. Police work has become much more complex and demanding than when I started, and it should no longer be seen as a blue-collar job. We want people coming into the organization with skills appropriate to meet the many challenges they'll face.

We also have to do a much better job of vetting. Pre-employment screening is so important. You want to avoid hiring tomorrow's problems. Major educational institutions could help in that regard by developing improved psychological tests. We're still using the same tests that have been used for decades, and many police departments conduct inadequate background tests.

There is no question that the police, in my view, are being less proactive because they've been getting many signals that if they take action and they're proven wrong, their job is at risk. We see less intervention on the part of officers, and that, in my judgement, is why we see violent crime going up in many major cities.

It is going to take time to get police in some places back into the mode of the prevention of criminal activity. They have backed off from proactive policing in many places because they're concerned about putting their livelihoods and family's well-being at risk.

Communication with the community is always important. We need to create teams in police departments that include community leaders who can work with officers to devise a problem-solving agenda and follow through on its goals. For instance, this may mean more enforcement actions should be taken – it's more than just shaking hands. It's collaboration that works.

Better education for police officers, body cameras, and working more closely with meaningful community groups can make a difference.

Elevating awareness of the dangers of cyber intrusion to the highest levels of the company is an important focus.

Did you know early on that you would end up in public service?

Not really. I was going to Manhattan College full time and was working as a stock clerk at Macy's part time. I read about the new police cadet program and I signed up.

I began working in the communication division of the NYPD. I worked on the switchboard and occasionally we would get emergency calls and handle them. Policing became very exciting to me.

When I graduated from college, I received a commission as an officer in the United States Marine Corps. At the same time, I also became a New York City police officer. After serving on active duty for three years, including a year in Vietnam, I returned to the police department and began going to law school on a part time basis. Perhaps the two experiences that held the most attraction for me in policing was first, the ability to make a real difference in people's lives and second, the excitement of it all.

In your law enforcement work, was it difficult to maintain a positive attitude with all the difficult situations you had to face?

There are some events I enjoyed and some that were quite painful. I'd sometimes have to notify a wife of a police officer that her husband had just been killed. Those are gut-wrenching experiences. I'd have to force myself to get back into a positive mindset before going onto the next challenge.

In high-profile public sector jobs, there is a lot of transparency and pressure. Every day is a new day. One can have plans to do something on a given day and, after reading the newspapers in the morning, have that agenda changed completely. This uncertainty is one of those things that makes being a police executive an exciting and challenging experience. ●