Teneo®

Insights

October 2017

Corporate Security and Risk Mitigation

Initial Lessons from Las Vegas

A discussion between William Bratton, Executive Chairman, Teneo Risk and Kevin Kajiwara, Co-President, Teneo Intelligence

William ("Bill") J. Bratton, Executive Chairman of Teneo Risk, and former Commissioner of the NYPD, spoke with Teneo Intelligence Co-President, Kevin Kajiwara, about the security implications and the key security considerations for corporations and businesses that have unfortunately been pushed to the forefront of every leader's agenda in the aftermath of the mass shooting in Las Vegas. Given the dizzying array of potential risks corporations face in today's chaotic environment (the new "normal"), Bill and Kevin discuss how corporations should be thinking about risk and security, and what can be done to guard both physical and reputational equity in an unpredictable world.

Kevin Kajiwara (KK):

To kick-off, I would like to introduce Commissioner Bratton to lay the ground work and set the stage for today's security and risk environment and give a general overview of how he is thinking about this and to define the parameters of the issue.

William Bratton (WB):

When it comes to crisis, it's not "if," it's "when." That's the one certainty that emerges from the uncertainty around us as we anticipate, mitigate, and navigate risk. We know this because it's always been thus. Risk and uncertainty are intertwined, and both can occasion fear. But navigating risk is made a lot easier by anticipating and mitigating it. So, although I acknowledge that non-economic risk, like economic risk, caries the caveat "past performance is not indicative of future results," keep this in mind: Awareness trumps fear, and preparation can turn risk into opportunity.

Whether contemplating the domestic and international threat picture, assessing the vulnerabilities of critical infrastructure, or planning how to respond to those crises that inevitably arise, CEOs and other leaders have to stay focused on thinking about strategic goals; and strategic thinking means seeing around corners.

Looking around the corner to 2018, I can't give you granular predictions. But I can give you this; 2018 will see:

- more acts of terror, and the methods and motives of terrorism will continue to expand;
- more civil disorder, because our strained polity will continue to fray amidst social and political turmoil before the civic garment is ultimately repaired;
- new international risks, as well as familiar perils, as America's ways of engaging the world continue to shift; and
- evolving cybersecurity threats that will continue to consume more and more corporate resources.

For each of these, and for the myriad of ways, large and small, that they may evince themselves and impact companies and leaders, we need to be prepared. Each constitutes a potential crisis, and for non-economic risk, crisis involves people's safety. Your company is nothing without your people, and they're counting on you.

Kevin Kajiwara:

Thank you, Commissioner. That was a sobering assessment of the world out there.

William J. Bratton
Executive Chairman,
Teneo Risk, New York

Kevin Kajiwara
Co-President,
Teneo Intelligence, New York

If I were to distill down the message that you're sending, it is that planning is critical for companies when it comes to risk mitigation and security measures. General Eisenhower famously remarked that, "Once the battle begins, the plans goes out the window," insinuating that plans are worthless. But planning, and the process of planning is actually everything.

I want to focus on the concept of planning ahead, as you described it when speaking to corporate leaders around the country and around the world. In general, how do you think Corporate America is doing on this front? Are they doing enough when it comes to security planning? And secondly, and maybe the more important question is, what's the starting point? How should companies really approach thinking about the issue of security in this strategic and conceptual way that you're talking about?

William Bratton:

This is a good news, bad news story. Some companies do an extraordinary job, in the sense that the issue of corporate security is dealt with at the highest level, but some companies do not address these issues as thoroughly as they should; the location of the security office in the basement, the location of the person responsible for security of the company being buried in the bowels of a division, where that is not being prioritized. I think the good news out of all these crises that I've just outlined is that increasingly, companies understand the potential for reputational damage, the potential for loss of life, the potential for loss of profits, and this new understanding is requiring that they focus much more attention on this issue, and that they elevate the responsibility and placement of, for example, a CIO, [putting them] much higher in the organization than has been the case in the past. That is something I certainly would advocate that all companies begin to think about doing.

Speaking from my own experience in the NYPD and LAPD, the areas of intelligence and counter-terrorism were not major priorities before 9/11. Post-9/11, the NYPD, with its now almost 2,000 police officers who focus on counter-terrorism intelligence areas and the LAPD with a proportionate amount, are reflective of how public safety had to realign and prioritize their resources.

What I would advocate for is that corporate America act in turn and recognize that this issue is as important as anything else that a CEO or the C-Suite, General Counsel, Board of Directors and CSOs have to face and respond accordingly.

Kevin Kajiwara:

One of the issues that comes up here is that, when we discuss security threats and security-related matters, there's a national tendency to think about all of the measures that could potentially be taken. But if companies were to follow through, in a literal sense, with each of these prescribed measures, you would end up building yourself an armed fortress. And many corporations have to be wary of balancing security with accessibility.

Thinking about Vegas, the entire city's economy is essentially predicated on its openness to the tourist trade—and not just in a one-off kind of way - they bring in large groups of people at any given time, and the openness of each individual resort, and frankly, of the city itself, are critical to the success of it.

How should companies be thinking about this: how to balance the security that's evident to your employees and customers, and to the potential bad guys, with the accessibility required to meet your business objectives?

William Bratton:

The use of the term balance is very appropriate to this discussion. In democratic societies, and speaking very specifically about the U.S. and Canada, freedom, accessibility and minimum intrusion of government are a source of pride and openly celebrated aspects of democracy.

However, more specifically, you tend to find experience effectively shapes and forms the reality of any city (or other specific area, location, individual, etc.). In New York City, with most buildings and other corporate entities, you cannot get in without at least going through some form of identification check, and that is a direct result of 9/11.

By contrast, I was amazed when I went to Los Angeles in 2002, within a year of 9/11, how lax the security was in America's second largest city. So, part of what we are facing now as we go further into the 21st century, is the idea of keeping a balance, and the balance of awareness, not fear.

I painted kind of a dark picture earlier, but that's a picture of awareness. So, I'm not living in fear, but I am certainly aware; and the awareness component is critical.

Having recently spent time in Las Vegas, that environment has to have accessibility. And so, this is where there are significant benefits from utilizing technology. There is so much that can be done through cameras, facial recognition systems, and other similar forms of security/intelligence tools. And this kind of technology is constantly evolving, and doing so at a rapid pace. This is where the awareness comes in. If you are, for example, a security director, staying abreast of changing technologies should be part of your daily job responsibilities.

Properly utilizing this technology allows for a smart, subtler method to increase awareness, and also, in some respects, to reduce fear, by understanding that having such parameters in place can reduce future occurrences. New York City is a case in point; since 9/11 there have been almost three dozen unsuccessful plans or attempts to [conduct] a terrorist act in the city. So many foiled attempts are largely a result of the intelligence, awareness, planning and technology that New York puts into its counter-terrorism efforts, but done in a way that still allows people to live their lives, and businesses to operate effectively.

Kevin Kajiwara:

Companies are thinking a lot about protecting their assets and their employees and their customers in the places where they do business. Businesses put their employees forward a lot on business travel, as well as conference and the like in places like Vegas, Florida, or New Orleans, and any other number of places where events can happen where you don't have the same control over the security environment that you might in your own home operation. So what about that aspect of protecting your employees as they are traveling on your behalf?

William Bratton:

There are multiple responsibilities both for the company and for the employee. The idea being that the company has an obligation as it sends people around the world, if they are moving into areas of concern, to brief employees about those concerns and increase their awareness of how to move and operate safely when in a foreign place. And more broadly, to have specific protocols in place, and clearly communicate what those protocols and plans are to employees, and provide employees with proper tools to follow these parameters.

There is also responsibility on the part of employees so, in a city like Las Vegas for example, if you are there on business for a company, and such a horrific event like the recent shooting were to occur, you follow your company's emergency protocol, whether it is to call back to the company as soon as possible, to make them aware that you are secure, that you are fine, you are safe, or if you have need of assistance—those things would be the duty of that employee. These are very simple things to do, and very necessary things to do—with the company responsible for putting those parameters in place, and the employee in terms of adhering to those protocols.

Kevin Kajiwara:

So, after an initial event occurs, your first order of business is trying to secure the situation with your employees, your customers, your assets. The second is protecting corporate reputation. I'm wondering if you have thoughts about incorporating as part of the planning process, how one would go about protecting reputational equity. And I'm also wondering, are there special issues that arise for companies who are iconic brands, as opposed to companies that are, say, substantial but perhaps more in the background in terms of public consciousness, and therefore not as attractive targets?

William Bratton:

Dealing with those issues is multipronged. Say you are a very recognizable Fortune 100, Fortune 500 company that has operations in multiple locations. In that case, social

media monitoring (similar to what is done in the police world) meaning, constantly scanning social media for events, public events, for example, may provide key insights and actionable information about groups that might be seeking to organize demonstrations around those events.

Similarly in the corporate world, particularly in cooperation with the police, New York City works closely with almost 3,000 corporate directors so that in the case of an event that will have a sizable impact (terrorism, demonstrations, etc.) local police can coordinate with local security directors from those companies to be aware of, and take necessary precautions if in fact either the companies, facilities or personnel are going to be in the vicinity of a demonstration, not directed against them - peripheral to it but still potentially impacted by it.

Awareness once again is important in these instances to take necessary precautions, and strength in relationships and collaboration with, for example, local police, can be hugely beneficial to corporations.

Kevin Kajiwara:

Since you've been on both the corporate and on the law enforcement side, I'm wondering what you think is ideal, particularly at a Fortune 100 level, in terms of corporate law enforcement relations as it relates to this kind of preparedness and keeping up to date with best practices, and just having that channel of communication ready to go in the event when things start to unfold very, very quickly and get very confusing.

William Bratton:

I'll use one word to answer that question: collaboration. Based on both my corporate and public-sector experience, I have learned that in order to survive successfully in dealing with potential security threats in the 21st century, no corporation can stand as an island independent from the rest of the corporate community, or in dealing with public safety world.

Leaders in both the public and private sectors need to communicate and constantly share experiences, share insight and share best practices so that we're constantly learning from each other.

New York, for example has an organization called NYPD SHIELD, comprised of thousands of corporate security directors in the Tri-State Area, who are networked into the NYPD. So, if a threat (a protest, a terrorist threat, etc.) is directed towards a particular entity that is part of this organization, that entity certainly would be closely working with the NYPD, but that piece of news would also be shared throughout that corporate community for greater awareness, so that everybody can help to prepare and to defend against it.

Going it alone in today's world effectively means you're going to perish. And so, with the corporations I advise, I constantly encourage collaboration; it should be the mainstay of both the corporate world and the public safety world, and is key to surviving in these uncertain times.

Kevin Kajiwara:

We talked about the security of one's own business and premises and the like, and spoke a bit about employees who are off premises and how to protect and make sure you're aware of their situation. But a lot of the businesses out there are multi-national corporations that don't just exist in and of themselves, but they are either the endpoint or a midpoint in a global supply chain with partners.

As one thinks more expansively, where a company's reputation and people are also aligned with something like an international supply chain, how do you – especially outside the country where your main jurisdiction is – how do you go about incorporating that into your risk planning?

William Bratton:

I think the idea of vetting any entity that's engaging with your corporation, and also increasingly, the idea of setting certain standards for any entities your company is engaged with, as it relates to representation of the larger corporation—and

more specifically, the idea that a corporation certainly should require that any entity that's working with them needs to adhere to and maintain certain standards—is important. Putting these measures in place reduces the vulnerabilities and exposure that naturally comes along with the association with a vast network or supply chain. Because, at the end of the day, in the event something does go wrong, the entity that's going to suffer the most reputational damage is the parent.

Many of the corporations that we advise don't function entirely on their own. They are very dependent on many, many other companies that they have to interact with. In such an interconnected world, companies are exposed to a greater degree of risk, and this particularly relates to the vulnerabilities that exist concerning the cyber world. Seventy percent of cyber intrusions are effectively the result of employees within the company or vendors that company is dealing with – so this proves the point that the vulnerabilities in today's 21st century world have significantly increased.

Given these factors, there needs to be constant reinforcement of standards of security as it relates to movement of invoices, contracts or other important and sensitive information, through the technology and cyber systems of these various companies. It is part of this overall idea of awareness that I keep talking about, and the sense that things change so quickly in today's business environment and it's certainly difficult to stay up to speed with information, technology, etc., but companies must strive to keep up these standards and be aware that they are affected by everything else they touch, whether that be another organization they partner with, or hire, or an individual person that works either internally or externally for the company. This is where the collaboration and awareness comes in; awareness of your connections and exposure, and collaboration with those connections where partnerships and working together are beneficial.

Bottom line with collaboration: I don't care how big you are, you cannot do it on your own, there has to be relationships that you have at all levels of the company, as well as partnerships externally, to ensure that you are doing all you can to stay on top of the security and risk issues that matter.

Kevin Kajiwara:

And what is your specific guidance for this? Corporations and boards are looking at very daunting cost on all of this, so what is the approach that one should take in order to make sure that they are spending in a responsible and reasonable way that is commensurate with the level of risk that you are outlining?

William Bratton:

The idea is to understand the exposure when you do nothing. This is an area that traditionally companies in the 20th century try to minimize to a great degree or have accepted certain losses. In the 21st century, we need to think differently, because failure to safeguard, failure to plan, failure to have policies and procedures in place both for prevention, as well as capability to respond, will lead to a much greater loss (reputational, financial and otherwise) in the long-run.

Kevin Kajiwara:

Companies are facing a dizzying array of potential treatments and options in terms of how to mitigate against threats, how to collaborate and how to plan and prepare. And I think that to some degree, it's very easy for businesses and their leaders to become like deer caught in the headlights when presented with the overwhelming list of choices. So, if you're a CEO who, in the wake of Las Vegas, is just sitting down with your CSO, your COO, your General Counsel, head of H.R., CIO, all the CXOs, etc., how do you begin the conversation? What's the starting point for the CEO here?

William Bratton:

Ed Koch, the former mayor of New York City, had a favorite expression that he was known for when he would meet constituents, business leaders or anybody else, "How am I doing?" Well, if you're a CEO (myself speaking from the perspective of a former commissioner role) and an event occurs, paraphrasing "How am I doing?", "How are we doing?", "Could this happen to us?", "Are there things that we could be doing to prevent this from happening to us?", are important questions to ask. They embody the proper state of mind leaders should be in, given today's risk environment.

And this is why I think that crisis actually provides opportunity. Crisis can obviously be looked at as a glass half empty scenario, but I don't encourage that at all. Crisis should always be looked at as the glass half full, if you will, because you learn so much coming out of a crisis. The learning experience out of Las Vegas, the unanticipated, the unexpected, the horror of what occurred there, out of this will come phenomenal learning opportunities for both the public and private sectors: the police, the hotel industry, those that engage in and plan major events.

So, it's the idea of constantly asking, "How am I doing?", and more importantly as a corporation, asking "How are we doing?", and learning from past experiences, and applying that learning going forward.

For more information on Teneo Risk and Teneo contact:

teneoinsights@teneoholdings.com

Teneo®

Teneo is a global advisory firm that works exclusively with the CEOs and leaders of the world's largest and most complex companies providing strategic counsel across their full range of key objectives and issues.

Comprised of the most senior talent, we work collaboratively to solve the most complex issues. Our teams integrate the disciplines of strategic communications, investment banking, management consulting, business intelligence, talent development, digital analytics, corporate governance, government affairs and corporate restructuring to solve for the most complex business and reputational challenges and opportunities.

The Firm was founded in June 2011 by Declan Kelly, Doug Band and Paul Keary and now has more than 670 employees located in 17 offices around the world.

teneoholdings.com