Jeremy Kroll Delivers Speech on Cyber Security and Risk Management

October 22, 2014
Contact: Michael Eisenberg, 212-694-7000

COLUMBUS, OH – Jeremy Kroll, Co-Founder and CEO of K2 Intelligence, delivered a speech at the launch of the Risk Institute at the Ohio State University’s Fisher College of Business on the cyber threat and the implications for Risk Managers, Boards of Directors, and Corporate Officers. Below are his remarks as prepared for delivery:

“We at K2 see risk management as a three-pronged proposition: risk prevention, risk mitigation and risk transfer.

“We see ourselves as helping to diminish and prevent risk before a corporate decision is made, taking proactive steps before a problem surfaces, and then also investigating incidents and implementing reactive measures to protect an enterprise after the fact. We also help mitigate risk after an incident has occurred. So we are involved at every step of the risk management process.

“We have partnered hand-in-hand with insurance companies in the past as part of a series of risk transfer joint offerings, and I will give examples of that later on in this discussion. We believe that the solutions that we provide to our clients are highly complementary to risk transfer products.

“Just to give you a bit of history about our company K2 Intelligence, it was started by my father Jules Kroll and I a few years ago after we left our old company Kroll Inc. A driving force behind the founding of our new company was that we were seeing the further acceleration of globalization and the ascendancy of the internet and all manner of information and economic activity being digitized.

“In parallel, we were also seeing several exciting and innovative cyber defense and Big Data Analytic tools that had been coming onto the market from the national security space over the last decade. We knew that these platforms had the capacity to revolutionize our business.

“These developments brought with them changing risk profiles for companies. And that meant that risk management models and methods needed to evolve to meet these new demands.

“Our industry had to do a better job of adapting to this new risk environment and harness these emerging technologies. We use Big Data tools to generate new insights, surface anomalous behavior patterns, and profile company risk within large and complex data sets.
“Many of the problems we have seen our clients facing over the years have remained largely the same. Companies still need to vigorously mitigate against insider threats, they still need to diligence investment opportunities around the world, they still need to protect against fraud, and they still need to comply with regulatory enforcement actions.

“But what has changed is the scale and scope of the issues that threaten corporate interests. They have grown dramatically over the last two decades. And we have worked hard to make sure that the scale and scope of our solutions have kept pace.

“When financial institutions are required by regulators to do forensic look-backs of billions of financial transactions, or a major retailer is breached and millions of customer records are stolen, more sophisticated solutions are needed to manage and mitigate those kinds of risks.

“We view ourselves as on the operational side of the risk management and risk transfer coin; the pointy tip of the spear, if you will, to help prevent and mitigate risk.

“In the cyber security context, we do this through intelligence gathering from within hacker communities and forums buried in the dark net. We do it through ‘social engineering’ training for executives, Boards and staff. We do it through helping to create response plans. And we do it through physical security audits, and forensic investigations aimed at boosting data protection procedures to mitigate against data loss, IP theft, and fraud. All of this is aimed at reducing a company’s exposure to cyber risk.

“The cyber threat is one of the most serious and is one of the newest threats confronting risk managers, Executives and Boards of Directors. At its heart, it is all about theft. The theft of credentials, the theft of economically valuable data, the theft of intellectual property, or just good old-fashioned theft of money. And this theft can also have major repercussions for a company’s brand and reputation.

“Let’s talk about the Insider Threat. Co-opting an internal actor, or breaching an organization through weaknesses in its defenses, is really just old wine in a new bottle. This kind of criminal activity used to be accomplished through blackmail, coercion, bribery, and other means and these same means are now being employed in new ways.

“Bloomberg recently reported that American companies and organizations suffered 40 billion dollars in losses from unauthorized use of computers just by employees alone last year. And the average annualized cost incurred by U.S. companies from cybercrime has doubled in the last 5 years, according to HP.

“Let’s face it, insiders have the greatest opportunity to commit these crimes. They have access to sensitive information, valid credentials, and access to the company’s enterprise cloud and other servers. It can also give a company’s competitors an advantage if an employee shares valuable information with them or take it with them to a new job.

“But the crimes themselves have not changed. Employees, 3rd party service providers, and supply chain partners have been stealing and defrauding companies since well before the advent of the internet and cybercrime.
“It is the ease and profitability of carrying out these kinds of crimes that has changed as the battlefield has shifted to include the digital world. We need look no further than Edward Snowden, who stole more than a million documents by downloading them onto a few thumb drives. Before digitization, he would have only been able to carry files that he had physical access to out of the office or try to make copies. It would have been a lot harder to inflict the kind of damage he did in a pre-digital age.

“Identity theft and theft of a company’s IP are also nothing new. We have been dealing with these twin threats for decades. Possible targets have always been myriad for these kinds of crimes.

“The insider threat, or even just employee negligence, such as opening the wrong email or leaving a laptop in a coffee shop, can lead to disastrous security breaches and the theft of valuable company information.

“That is what we continue to hear. That at the heart of it all, companies are worried about people and bad behavior. The technical components are just the medium through which these crimes take place.

“The business community has been shifting from trying to erect the tallest walls and widest moats around their systems, toward an emphasis on preparation, containment and mitigation. They are looking for solutions that can reduce their risk exposure. They understand that it is no longer a matter of ‘if’ but a matter of ‘when’ they will be compromised.

“Many companies are now working for the first time to put together their cyber incident response plans. C-Suites and Boards are increasingly asking questions like, ‘How should we handle a breach internally? How should our GC and other senior leadership be involved? When do we notify our attorneys? When do we disclose the breach publically to investors, to regulators, to customers?’

“Having good answers to these and many other questions is becoming a major component of risk management and, more importantly brand management, for almost every company.

“One example of a solution that we offer is we have a team comprised of serious cybersecurity practitioners who came out of elite government cyber units around the world. We operate extensively inside the gray and black hacker markets and forums known as the ‘dark net.’

“The dark net can only be accessed with the help of specially designed anonymizing software and requires a significant amount of familiarity and expertise to navigate.

“This is the staging ground, the safe haven, from which the most sophisticated cyber criminals launch their attacks. This is a place where cryptocurrencies such as bitcoin are the coin of the realm. Stolen data, attack kits, zero day vulnerabilities and many other valuable products that have been procured illegally are bought and sold inside this dark market.

“Since this market has no physical boundaries, our team can access these closed communities from anywhere in the world and can cover huge swaths of virtual territory. So while hackers can operate and transact business with relative impunity inside of this borderless marketplace, it also provides an advantage to our team as well.
“We speak sixteen different languages. We know where to find the cyber attacker tool kits, the how-to guides to defraud companies, and the compromised employee and customer information that can be used to penetrate a specific company. We also know how to interact with hackers in these forums to extract intelligence.

“So we deploy these assets to provide our clients with a highly sophisticated cyber intelligence solution. We outline for clients what hackers are saying about them, what targets they are casing, what data has already been exfiltrated, and what information attackers already have to exploit the weaknesses of our clients’ systems and personnel. Information like this can allow companies to be more prepared and have a fuller profile of their risks and their vulnerabilities.

“Also, there is an awareness gap that many companies have around what data they actually possess. They may not know where their valuable data is located, how it is formatted, who has access to it, or how to secure it. Many times this is as a result of maintaining legacy systems, importing data that came to the company through acquisitions of other companies, or even from outdated equipment.

“Corporations are also looking to understand how a malicious insider or an external actor might try to penetrate their systems and their supply chains, as well as what data they are likely to exfiltrate.

“Behavioral and predictive analytics tools can model and surface anomalous and suspicious behavior, as it emerges, and can also help mitigate against the insider threat. Bad behavior leaves an electronic exhaust and it needs to be understood in order to grasp what potential risks are emerging and how to best protect against them.

“In the age of spear-phishing attacks and diffuse supply chain vulnerability, fortifying a perimeter with guns, guards and dogs and having a small siloed team devoted to security just won’t cut it anymore.

“Every person in an organization is a potential gateway for an attacker. That means that every employee and 3rd party needs to be enlisted in the effort to protect the company, and ultimately the brand. There needs to be an overall culture of security that starts from the Board of Directors and permeates all the way down into the rank-and-file.

“That culture may even need to be pushed down by senior management and the Board if it is not widely adopted. Pushing down that culture of vigilance and security can be a considerable challenge, and is something that many companies are wrestling with. However, it is critical to maintaining a robust security posture.

“Employees need to know when not to click on a specific email or attachment, and they need to be on the lookout for other types of sophisticated social engineering attacks. It is not enough for them to just take that company training course once on their first day of employment or once a year. It needs to be re-emphasized and social engineering training should be ongoing.

“To illustrate the dangers of some of these social engineering attacks employed by cyber criminals, I want to talk about a new term of art out there to describe a certain kind of phishing attack, called ‘Whale Phishing.’

‘Whale Phishing’ describes a specific kind of plot that targets senior company officials, hence the term ‘whale.’ The credentials of a senior company leader are spoofed and then an email is sent from their address to a mid or lower level
employee in the finance department with access to banking funds but who does not typically have much exposure to senior corporate officers.

“We have seen several variations of this kind of attack. In fact, one of our senior team members recently helped a client, a major manufacturing company, deal with a sophisticated “whale phishing” scam.

“In this case, a mid-level member of the finance team received an email, purportedly from the CEO of the company that was described as ‘highly confidential.’

“The employee is told in an email from the CEO that he is working on a very confidential deal and that he needs to have two million dollars wired to a specific bank account at a well-known major bank, care of a particular Chinese company that does in fact exist.

“This took place during an opportune time, because, while all of this was going on most of the finance team was at a 3-day off-site meeting.

“The email instructed the employee that he shouldn’t talk to anyone else inside the company. He was told that if he needed to talk to someone else, he could talk to a senior partner at a Big 4 accounting firm and the email included contact information for that individual. He was told specifically not to discuss it with his immediate supervisor.

“The employee checks to see if there was a partner with that name at the Big 4 accounting firm, which there was. And then, he starts going through the process to cut a check for two million dollars and the first payment goes through. During the next 24 hours, the employee is communicating back-and-forth with this impostor CEO.

“Then the employee gets another email from the impostor CEO, acknowledging receipt of the first payment and asking for an even larger transfer, approximately six million dollars, into the same bank account. Then there was a third and final transfer. All told, the employee wired out over eighteen million dollars of company funds in a 72 hour period.

“When the finance team gets back to the office from their off-site and discover all of this activity that is when questions start being asked. They go to the employee who authorized these transfers and he tells them that the transfers were all at the direction of their CEO.

“That is when the real, non-impostor, CEO hears about all of this for the first time. An attempt was then made to try and force a stop-payment but the account had already been emptied out.

“After all of this took place is when our team member was contacted. He was asked to find out whether it was a data breach, collusion with a malicious insider, or some other problem. It turned out, as we now know that this was a case of a ‘whale phishing’ attack targeting a negligent employee.

“And the timing was highly suspect, since all of this happened during a 72-hour window when most of the finance team was away. This is still an ongoing matter so there are still a number of unanswered questions. However, it has all the hallmarks of
a highly sophisticated Advance Persistent Threat, or APT, attack using social engineering techniques to steal millions of dollars from the target company.

“Spear-phishing is not limited to preying on mid-level employees in the Finance department. An attack from a few years ago that has been publicized selectively in the media targeted CEO’s directly.

“It was designed to trick them into clicking on a malware link by sending them emails from an email address that looked like it was from federal authorities. The email would inform the CEO that they were being subpoenaed and prompted them to click on a link to view the subpoena.

“Anywhere from fifteen thousand to twenty thousand emails like this were reportedly sent out to different CEO’s. And an astounding ten percent of those receiving the email clicked on the malware links. That is nearly two thousand Chief Executives who fell for this scam and compromised their own systems. And these attacks have only grown in sophistication since.

“Another piece of the cyber risk management puzzle that we cannot forget about is the physical security piece. Too often we see examples of companies who have strong cyber defenses but anyone can walk in off the street, right through the front door, and into their offices without being stopped by anyone.

“Just because real-world theft is less in the headlines these days, doesn’t mean it can be ignored as a risk. Laptops and smartphones can be stolen. Sensors and cameras can be disabled if not properly defended. Malware-infected thumb drives can be plugged into systems by negligent employees.

“At the end of the day, we still live in a physical world. Again, we need to have that overall culture of security in place for the entire organization, not just the IT team.

“Speaking of the IT team, they can oftentimes be another source of risk that may need to be managed. They have the potential to be some of the most dangerous insiders due to their intimate knowledge of a company’s systems.

“We had one client recently that laid off several members of their IT team. Shortly after, disruptive actions started taking place. Files began disappearing. Printer and email servers were deleted. And fictitious emails were sent to and from the senior management of the company, including the CEO.

“We were called in to identify the attackers, investigate how they got into the company’s systems, prevent any further damage, and gather evidence to support civil and criminal proceedings.

“We profiled their system and determined that they had not been hacked. The fired members of the IT team had left the company with both access to the system and had planted a variety of remote desktop packages. These packages allowed them to have unhindered access to systems and do illegal surveillance of employees.
“We ended up fighting off the attack in real time just as we were called in to provide assistance. At one point, our team was actually fighting against the attackers by pushing their cursors away from accessing certain files. I would call it a ‘cyber duel’ of sorts.

“We shut down the instances of remote software and blocked the attackers’ access to the company’s system.

“Now once these malicious former insiders were thwarted by our team in cyberspace, they attempt a physical break-in. One of them broke into the IT building with a stolen pass and hooked up a computer to the company network to download more remote PC software.

“The break in was spotted the next day when the perpetrator tried to access the systems again. We reviewed Closed Circuit Television feeds and removed the hidden PC and software.

“This example throws into sharp relief the kinds of threats and risks that companies are facing every day, especially from malicious insiders and former insiders. It also shows why the best practices and procedures around physical security risk management are so important to build, test, and strengthen.

“From where we sit, we are starting to see the cyber risk transfer and loss control business really begin to take shape. Cyber insurance as a product is evolving and there are now richer data sets from which insurance companies can write policies.

“I have to say that, from our experience, demand is also on the rise. According to new data, the percentage of companies holding cyber insurance policies has risen from ten percent in 2013 to twenty-six percent this year, according to a survey done by the Ponemon Institute. The financial services sector experienced the largest increase.

“And while that is still a fairly low percentage, it does show that uptake for this product is growing. Travelers Insurance estimates that current U.S. premiums for cyber insurance is at around 1 billion dollars, and it won’t be long before it reaches 2 billion dollars.

“Target recently reported at least two-hundred and thirty-five million dollars in expenses related to its 2013 breach, with some estimates putting that number as high as four hundred million dollars. And they were reportedly able to recover ninety million dollars of that under their cyber liability insurance policy. The hit to their market share as well as their brand, was massive, and is still growing.

“Insurance coverage for this threat is an essential part of any comprehensive cyber risk management plan across all major industries. Executives and Board Members are now coming to terms with the potential financial damage a large data breach can inflict.

“Cyber liability policies are becoming more readily available in the marketplace and we believe they offer a critical layer of protection. Insurers are asking for ever-more detailed information and documentation about a potential customer’s information security. This is a very positive development because it fosters necessary dialog and better cyber hygiene.
“It pushes companies to implement many of the practices that cyber insurance questionnaires ask about, whether it is developing a formal Incident Response Plan, putting in place heightened protections around access control and encryption, conducting penetration tests, or creating robust data recovery procedures. It also forces the needed integration of physical and cyber security.

“Our company has a history of working with insurance companies as partners in the provision of certain kinds of specialized insurance products. We sold our old company, Kroll Inc. to Marsh & McLennan, which was obviously a big decision for us at the time. But we felt that our business was a good fit within the insurance context as part of the solutions and advice offerings for Marsh’s customers.

“So, when my father Jules and I were at Kroll we forged a partnership with AIG to provide personal security services to high net worth individuals and their families in AIG’s Private Client Group.

“One terrific example of this was, we would evaluate a customer’s data usage habits and then offer programs specifically designed to mitigate the risk of electronic identity fraud and other electronic intrusions. Pretty much anything that related to theft of identity or personal information that could compromise customer assets and personal security.

“And keep in mind, this was in the late 90’s and early 2000’s, well before the massive and frequent data breaches that we see proliferating today. In today’s context, intra-industry partnerships, like we are seeing with Information Sharing and Analysis Centers (or ISAC’s) are a very encouraging development for cyber risk mitigation. ISAC’s are forming for many major industries, from Real Estate to Aviation, from Maritime to Surface Transportation.

“However, more needs to be done to work across industries to foster even more cooperation and information sharing. Combating a threat that is this pervasive will require all of us working closely together across the economic landscape.

“Look, these are uncertain and difficult times that we live in when it comes to combating the cyber threat and reducing the risk of an incident. In a lot of ways it is a very exciting time to be in the risk management business too.

“That is because we get to play a role in shaping what the new cyber risk mitigation and transfer strategies will look like in the future. We get to help define a new market in interesting ways.

“It will take all of our collective efforts, and all of our collective creativity, to develop the strategies and products that our customers and clients are asking for. They are looking to all of us in this room to provide them with the solutions they need to manage cyber risk. And I look forward to working with all of you to help develop them together.