BlackBerry Cylance on the Future of Proactive Cybersecurity

Information security veteran emphasizes the need to move past a detection-based model to a mathematically predictive model.

Adam Patterson

Fri, 07/19/2019 - 11:59

John McClurg, vice president and ambassador-at-large of the Office of Security & Trust at BlackBerry Cylance talks future of security. Photo Credit: Geoff Livingston

Cybersecurity in the U.S. is moving beyond a reactive model to an era of proactive prevention, noted a security leader at cybersecurity firm Blackberry Cylance.

Former FBI cybersecurity expert and Vice President, Office of Cybersecurity and Trust at BlackBerry Cylance John McClurg joined the State of Cyber CXO Tech Forum July 18 to discuss the origins of American information security as well as the future of the field. McClurg outlined a storied career in FBI counterintelligence and

cybersecurity, paying special attention to the origins of federal cybersecurity.

McClurg was brought to the FBI counterterrorism task force due to his background in hermeneutics, with recruiters particularly interested in his ability to help predict terror attacks and foster a culture of proactive security. He mentioned ongoing frustration within the U.S. intelligence community over post-facto investigation of terror incidents, mentioning that both the Lockerbie and Oklahoma City bombings were only scrutinized after the attacks.

"We were pretty much stymied in the world of proactive detection," he said at the event.

McClurg detailed that this focus on reactive detection was carried into the nascent field of cybersecurity as well. This resulted in a culture within the federal government where network breaches were only corrected after the fact, with a primary emphasis on damage control and repair. After extensive experience with both counterintelligence and cyber investigations, McClurg mentioned it had become abundantly clear that the U.S. had to move beyond this style of detection that risked considerable information compromise even in the case of relative vigilance. He tied this deficiency to underperformance in piecing together key indicators of data compromise, a vulnerability that allowed attackers to maintain sustained access to core systems.

McClurg mentioned that the advent of big data analytics provided a template for a more sophisticated threat detection and prevention system. After helping design an insider threat program within the federal government, McClurg retired to take his expertise to the private sector.

Toward proactive prevention, the most promising development in this field appears to be the leveraging of artificial intelligence, which has been McClurg’s primary focus at BlackBerry Cylance.

When McClurg transitioned to the private sector, signature-based antivirus programs were still the dominant means of detecting information compromise. Rather than relying on this as a fixed paradigm, McClurg helped analyze various known methods of data breach and use this as a means for better understanding the broader cyber landscape. He made a habit of leveraging these insights to prevent future attacks — extrapolating what they indicated about the threat landscape to foster a more proactive form of data protection. McClurg ensured this

became an ongoing cycle throughout his tenure in the private sector, a methodology that helped instill the foundations of a proactive, rather than purely reactive, cybersecurity culture.

McClurg noted particular success with first leveraging this style of cyber innovation at Dell, where he helped an information security team draw insights from the broader cyber landscape and run a complex array of zero day and ransomware attacks within a threat simulation model. The result was the successful diversion of over 99.7% of the simulated attacks — a significantly more effective mode of information security protection than the longstanding signature-based antivirus paradigm.

He concluded by outlining that mathematically predictive models represent the future of cybersecurity and that both the federal government and private sector would be best served by implementing these measures in lieu of the antiquated signature-based response method.

View printer friendly version
CXO Tech Forum State Cyber 2019
Federal Cybersecurity
predictive analytics
Data Analytics
Duplicate
Standard