Congressional Report Concludes CylancePROTECT® Played a Pivotal Role in Discovering, Stopping and Remediating Malware that Caused OPM Data Breach

Report shows artificial intelligence based security software was key to halting data breach in progress

Wagner also testified that Cylance was able to find things other tools could not "because of the unique way that Cylance functions and operates. It doesn't utilize a standard signature of heuristics or indicators, like normal signatures in the past have been done, it utilizes a unique proprietary method."[505]

Cylance tools later proved invaluable after 74 days of deployment to over 10,000 devices these tools detected almost 2000 pieces of malware on OPM's system and later blocked new threats. Unfortunately, the most effective preventative tool – Protect was not deployed until long after the attackers stole background investigation and fingerprint data and personnel records from OPM's system. The next Chapter describes the assistance another contractor provided to OPM during the 2015 incident response period.

In sum, Wagner's assertion that OPM did not deploy Cylance's preventative tool – Protect – sooner because it was not FedRAMP compliant is lacking given OPM's actions at the time in buying other non-FedRAMP compliant products.

OPM's Director of IT Security Operations, Jeff Wagner, testified that political reasons were not why OPM failed to purchase Protect. Wagner stated the primary reason that OPM did not acquire Protect was because "Cylance didn't currently have a FedRAMP-certified cloud."[595]

This raises a question as to why OPM did not purchase and deploy the tool sooner, in June 2014, when it may have been able to prevent or mitigate the attack, especially given the fact that OPM knew its most sensitive data was being targeted by sophisticated hackers. Documents and testimony show internal agency politics and procurement challenges made it difficult to quickly purchase and deploy security tools.

OPM's Director of IT Security Operations, Jeff Wagner, testified that political reasons were not why OPM failed to purchase Protect. Wagner stated the primary reason that OPM did not acquire Protect was because "Cylance didn't currently have a FedRAMP-certified cloud."[595]

On April 24, 2015, OPM upgraded Protect to auto-quarantine mode. At 4:11 p.m. on April 24, Coulter emailed several colleagues to announce the upgrade. He wrote:

> Guys - OPM hit critical mass today and **is burning the house** - literally! **They just hit 'global-quarantine' for every threat! I think it was around 1180 threats in the queue. This was done per senior orders**. They are also pulling the power on every device starting Saturday at 9am - Sunday at 5pm. I need everyone's help to make sure what they quarantined will not be mission critical files. I have been up for 24 hours so I really do need help.[555]