5 QUESTIONS FOR Eric O’Neill
THE FBI “GHOST” WHO BROUGHT DOWN A RUSSIAN MOLE

Carbon Black.
Eric O’Neill serves as Carbon Black’s national security strategist where he is a thought leader on a wide range of issues including counterterrorism and national security matters. Prior to this, he worked as an operative for the FBI, where he conducted national security field operations against terrorists and foreign intelligence agents. His recent book, Gray Day: My Undercover Mission to Expose America's First Cyber Spy, recounts his role in the investigation and capture of the most notorious spy in U.S. history, Robert Phillip Hanssen—a story which was also the subject of Universal Studio’s movie Breach, released to critical acclaim in 2007.

We sat down with Eric O’Neill to get his perspective on today’s threats and the state of cybersecurity.
We once filed documents in towering cabinets, coded and organized by secretaries who held the keys to the kingdom. Spies would loiter by bars near government buildings, waiting with friendly ears for evening alcoholics looking to complain about their boss or the bureaucracy. They would search out highly placed individuals who had a secret they wanted buried, those who had lost faith in America or those in financial distress who needed fast cash to make ends meet. After long recruitment periods that involved sham friendships, bribes, and often threats, these marks became the perfect inside men to extract the paper that held the secrets. But, as businesses and government agencies began to trade the file cabinets for computer systems and servers, cell phones and laptops, thumb drives and cloud based computing, spies had to evolve.

Today, there are no hackers, there are only spies. The hackers of yore have gone off to join cybersecurity companies or to found startups. Spies have stepped into the space left behind. They are intelligence service experts trained to use traditional spy craft to recruit individuals at targeted organizations and steal their access to information. These spies are sophisticated, devious, and well-funded—and they’re behind all of the major security breaches we’ve experienced this century.
As a young FBI operative, I went undercover to help catch Robert Phillip Hanssen, a 25-year veteran of the FBI who had been selling secrets to the Russians for decades. He was the most destructive mole in US history—and the first to take advantage of holes in the country’s cybersecurity infrastructure. Hanssen and I spent a lot of time together during the case, and he often pontificated about what he called Hanssen’s Law: “the spy is in the worst possible place.” What he meant was that spies will seek out the secrets that will do the most damage in order to sell them for the most money. The cloak and dagger espionage of the past and today’s modern cyber espionage share the common theme of proving Hanssen’s law correct. The only difference is in the methods of obtaining that information.

Hanssen taught me that counterintelligence is not won by defending against threats, but by actively hunting the spies where they hide. Decades of security work and investigations have proven my former mentor and target correct. If we don’t hunt the threats, they will hunt us. Our traditional, defensive approaches to cyber security that rely on protecting a perimeter are outdated, expensive, and fail against modern cyberattacks. We need a different playbook. Just as spies once took lessons from hackers, cyber professionals must become expert spy hunters.
Foreign cyberattacks and espionage pose the largest threat to US Security. Over the past two decades, Russia, China, North Korea, and Iran have all made massive investments in cyberespionage and the tools needed to launch disruptive and destructive cyberattacks against the critical infrastructure of rival nations. A recent February 2018 report by the Council of Economic Advisers to the Whitehouse pegged the cost of cyberattacks to the US Economy between $57 and $109 billion in 2016.¹ Each year the losses grow. The United States has made great leaps forward in our offensive and defensive cyber capacity, but foreign investments in attack ability continues to outpace the United States.

¹ THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY, FEBRUARY 2018
In my book Gray Day: My Undercover Mission to Expose America’s First Cyberspy, I speak at length about suspicion and paranoia. Threat hunting requires investigators to balance on the razor’s edge that separates suspicion from paranoia. Suspicion is healthy. It guards your back, keeps your eyes up and open and alert to signs of danger. Paranoia is suspicion’s ugly younger brother. Paranoia paralyzes decision-making, invents threats out of thin air, and crushes all confidence beneath a heavy boot. Cybersecurity professionals walk this same narrow line when hunting threats within the environments they protect. The key to success is continual suspicion of threat information that uses training, the best technology, collaboration with peers, and big data assistance to correctly judge threats from anomalies. Without assistance, cyber threat hunters can quickly fall into paranoia where decision-making is paralyzed by lack of information and everything looks like a threat.
Over the years since my time locked in room 9930 at FBIHQ with the worst spy in FBI's history, I've spent a great deal of time reflecting on the lessons Hanssen taught me about espionage's cyber revolution. In the years since, I've updated Hanssen's Law to fit our modern espionage problems. In my book Gray Day (as a nod to my old Boss) I call it...

O’NEILL’S LAW:
Hacking is the necessary evolution of espionage.
There are no hackers, there are only spies.
We must hunt the threat before the threat hunts us.
Because the spy is always in the worst possible place.
To learn more about Eric’s story, check out Carbon Black’s recent webinar:

GRAY DAY: HOW I CAUGHT THE MOST DAMAGING SPY IN AMERICAN HISTORY

Carbon Black.

© 2019 Carbon Black Incorporated. All rights reserved. Carbon Black and CB Predictive Security Cloud are registered trademarks or trademarks of Carbon Black, Inc. in the United States and/or other jurisdictions.