Christopher Paul Hasson

- US Coast Guard Lieutenant
- Former USMC and Army National Guardsman
- Secret Clearance (Declined TS/SCI)
- No previous derogatory information
- Acquisitions Officer
- 49 years old and married with two children

CDSE

Center for Development of Security Excellence

CASE STUDY

Targeted Violence

WHAT HAPPENED

Christopher Paul Hasson was arrested on February 15, 2019, which prevented him from possibly carrying out acts of violence. His arrest followed a multi-year investigation that included monitoring the use of his U.S. Government automated information system. He pleaded guilty in October 2019, and on January 31, 2020, at the U.S. District Court in Greenbelt, MD, was sentenced to 160 months in prison on four federal counts, to include three felony weapons charges and one felony drug charge. Hasson owned a residence in Silver Spring, MD, and worked at the U.S. Coast Guard Headquarters in Washington, D.C.

Hasson self-identified as a "White Nationalist" for over 30 years in writings advocating for "focused violence" in order to establish a white homeland. Review of Hasson's email accounts, saved documents, text messages, and Internet searches revealed he was inspired by racist murderers, stockpiled assault weapons, studied violence, and intended to exact retribution on minorities and those he considered traitors. He admitted from at least March 2016 through early February 2019 that he used various email accounts, including an overseas encrypted e-mail account, to order the opioid Tramadol from various illegal Internet-based distributors.

Hasson prepared to take action and used his government computer to read the manifestos of mass murderers such as Norwegian terrorist Anders Breivik, Unabomber Ted Kaczynski, and Eric Rudolph, the 1996 Atlanta Olympics bomber. He performed Internet searches and developed lists of potential targets, including media personalities and current and former elected officials. He conducted attack and targeting research and planning, and operational cover support activities. He imitated actions contained in some of the extremist manifestos listed above such as purchasing steroids.

INDICATORS

- Associating with extremist group or with individuals' espousing extremist views
- Expressing ill will toward U.S. Government
- Possessing illegal weapons and/or illegal drugs
- Misuse of U.S. Government automated information system

IMPACT

The Christopher Paul Hasson case was an example of a positive insider threat outcome in that an insider threat hostile act was prevented by an effective insider threat program, which included user activity monitoring that identified attack and targeting research and planning and operational cover support. The case highlighted a holistic approach and the successful collaboration between the organization's insider threat program and other agencies. Had his activities not been detected or detected in time, he might have been able to carry them out against some of the same individuals whom he researched and placed on target lists. The result could have been devastating.

Lastly the Hasson case illustrates the complex and unpredictable nature of human behavior and the fact an individual's thoughts or ideations are not transparent to others, making it more challenging to detect and report questionable or anomalous behavior. In his case, while having researched and shown an interest in white nationalism and other racist ideology, some of his past performance evaluations characterized him differently, even to the point of being an advocate of equal opportunity. This case also raised the issue of balancing safety and security with First and Second Amendment protections.

ADDITIONAL

Christopher Paul Hasson's performance evaluations characterized him more as an advocate of equal opportunity rather than a "White Nationalist." Hasson used his U.S. Government systems for many of his activities, to include research, purchases, and communications.

Consider the following questions:

- How can an insider threat program identify anomalous behavior?
- Why is User Activity Monitoring a part of an effective insider threat program?
- How do we balance the protection of First and Second Amendment rights with Safety and National Security?

Resources for further exploration:

- Insider Threat Indicators in User Activity Monitoring
- Insider Threat Privacy and Civil Liberties INT 260.16 eLearning Course
- Insider Threat Potential Risk Indicators

Supporting Through Reporting!

Contact the appropriate POC to report any observed potential risk indicators:

Name: _____ Agency/Department: _____
Title: Supervisor/Security Officer/ITP Senior Official/ITP Manager