2010-04-16

Data could help track potential insider threats

CHDS Staff

Data could help track potential insider threats

chds.us/c/item/278

The tragedy at Fort Hood taught that detection of an insider threat requires integration of data from multiple sources, both from within and beyond organizations. In the Technology for Homeland Security course, Michael Brown wrote a paper supporting a case for organizations to develop and implement knowledge management systems to strengthen the organization's capability to proactively detect potential insider threats and subsequently avoid an event with negative or tragic consequences.

"Unfortunately, there is no silver bullet that would provide any employer with the specific indicator, predictor, or tipping point that leads to an insider threat," notes Brown, who works at the Transportation Security Administration in Arlington, Va. "Therefore, organizations must examine how to convert data into information, and generate knowledge from that information, in order to develop the appropriate capabilities that can be used to detect those who intend to cause harm."

1) Brown's research was designed to identify examples of data points throughout an individual's career which, along with behavioral triggers such as tendencies of violence, threats to co-workers, or jihadist sympathy, could be used by an investigator to make a risk determination based on the totality of circumstances surrounding an individual. Such an employee lifecycle security assessment could be used to proactively initiate an investigation to validate or discount the existence of an insider threat.

2) Organizations can begin moving forward to close gaps by examining 'what' vulnerabilities exist and 'how' they can be exploited. Moving forward, the introduction of knowledge management systems provides organizations with an opportunity to leverage a different set of data points to identify 'who' provides the greatest risk to the nation's transportation systems from an insider threat perspective. Extracting data from different sources could highlight someone who presents a higher probability of doing something wrong than someone with no identifiable attributes.

3) The completion of Brown's paper has helped prompt decision makers to recognize the various points of data that can be used to detect anomalous activity by an insider with the intent to cause harm. Technology can influence the speed by which these data points are integrated and insider threat detection is recognized as an organizational core competency.

[Course paper not posted upon agency's and author's request]