National Risk Estimate: Insider Threat

The Department of Homeland Security's Office of Cyber and Infrastructure Analysis (OCIA)[1] Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) completed the *National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat* in December 2013. This National Risk Estimate assesses key security issues from malicious insiders to provide the critical infrastructure community with an overview of the potential risks and implications. OCIA used subject matter elicitations and tabletop exercises to project the effect of historic trends on risks over the next 3 to 5 years. OCIA also used alternative future analysis to examine possible future events from insider threats to critical infrastructure over the next 20 years. Taken together, the results of these analyses can assist owners and operators in understanding the scope of the risk and can inform mitigation plans, policies, and programs, particularly those focused on high-impact attacks.

The malicious insider threat is complex and dynamic, and it affects the public and private domains of all 16 critical infrastructure sectors. Owners and operators responsible for protecting our nationally-critical assets must recognize the nuances and breadth of this threat in order to develop appropriate risk-based mitigation strategies. Following is a summary of the key findings and recommendations from OCIA's analysis. To request the *National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat*, please email OCIA@hq.dhs.gov.

THE THREAT: MALICIOUS INSIDERS

- Access and specialized knowledge give insiders tactical advantages over security efforts.
- Technological advances, globalization, and outsourcing increasingly blur the line between traditional insiders and external adversaries.

Two major factors complicate efforts to assess and reduce the likelihood of malicious insider attacks:

- **The challenge of identifying and predicting the stressors or triggers that can cause a trusted employee to become a malicious actor; and**
- **A lack of detailed and reliable data on insider breaches and attacks.**

[1] In February 2014, NPPD created the Office of Cyber and Infrastructure Analysis by integrating analytic resources from across NPPD, including the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and the National Infrastructure Simulation and Analysis Center (NISAC).

- Insiders who combine advanced technological understanding with traditional espionage and terrorist skills have a significantly increased asymmetric capability to cause physical damage or disruptions through cyber means.

THE VULNERABILITIES: EXPANDING ORGANIZATIONAL SECURITY BOUNDARIES

- Sectors with relatively robust preventative programs and guidelines can still face a dynamic and expanding threat.
- Organizations are likely underestimating the threat from third-party insiders, such as vendors, contractors, and subcontractors.
- Industrial control systems in critical infrastructure are attractive insider targets for remote sabotage and espionage in an increasingly networked world.
- Without credible and sector-specific insider risk information, critical infrastructure owners and operators are likely to underestimate the malicious insider threat and make insufficient or misdirected investments in security.

THE CONSEQUENCES: ASYMMETRIC IMPACTS

- If the goal of malicious insider activity is exploitation rather than destruction of assets, it will be more difficult to detect, potentially resulting in serious cumulative consequences.
- The impacts of a targeted physical attack on critical infrastructure using cyber means could be much more severe than those of a conventional cyber-only attack.

RECOMMENDATIONS

- The Government and private sector should work to develop comprehensive and scalable insider threat program standards that incorporate long-term employee monitoring policies, including background checks and re-investigations, effective contractor and subcontractor vetting processes, employee training, and termination of access at separation.
- Effective prevention and mitigation programs must be driven by better understanding the insider's definition of success against a particular sector.
- Organizations should establish specific workforce behavioral and access baselines, and an understanding of hiring, oversight, access, and security policies, in order to identify anomalies.
- Employees used as a monitoring force may be an effective way to identify malicious insiders. To be effective, they must have access to recurring training.
- Public and private organizations must consider how to balance the best risk-based security procedures against the myriad of policy, legal, and employees' rights issues associated with obtaining and analyzing relevant threat data in the workplace, especially data derived from social media and behavioral monitoring.