Reducing Insider Risk Through Continuous Vetting

Summary of Roundtable, hosted by ATARC in November 2022

WHITE PAPER

Early detection of insider risk is a critical component to develop a proactive cybersecurity posture. Continuous vetting is key to a healthy workforce and efficient operations, but agencies often face challenges when developing insider risk programs.

In a recent roundtable discussion, the Advanced Technology Academic Research Center (ATARC) invited experts in the field to share their insights about the challenges and successes involved with implementing robust and agile continuous monitoring processes. Much of the discussion centered around the necessary components of an effective insider risk program.

The Search for Data

One of the leading components of an efficient and effective insider risk program is data. Policies designed to minimize insider risk set benchmarks for agencies to meet, while at the same time, agencies work to identify risk based on unique use cases. Because insider risk takes on many forms and can be influenced by many factors, such as agency culture, leadership style, economic conditions, and mission objectives, data collected to support insider risk programs differs from one agency to the next.

There are multiple perspectives from which to examine insider risk at an agency. Policies and regulations aimed to reduce insider risk are typically reactionary and prompted by an event. While policies are helpful and needed, roundtable participants urge agencies to begin looking at insider risk from a wider perspective. Certain economic conditions can sometimes trigger a rise in insider threats, but so can a shift in the technology preferences of certain generations. Leaders should examine whether they are looking at the right information to determine risk within their agency.

Capturing data to provide an accurate, complete picture of insider risk is challenging. Some agencies at the roundtable shared that they don't have access to all required data sources to create a complete picture of insider risk. Even the data sources they can access are often incomplete. Despite these shortcomings, roundtable participants recommend agencies to collect and receive data in a variety of ways, rather than collecting data to meet compliance standards.

Other agencies are challenged with knowing what analysis should be done to reduce insider risk with the data that is collected. Moreover, if agencies are collecting data and defining variables differently, then analyzing insider risk to identify government-wide patterns is close to impossible. Standardizing insider risk data is a critical, but challenging step to producing outcome data.

"Data is just data. It's not information. Insider risk requires information to make decisions. You have to combine the technology with people, because people are going to make the final decision."

Roundtable Participant

Ultimately, though, data is just data. It's not information. In order for agencies to transform data into usable intelligence built for insider risk programs, they must first

 info@atarc.org

define what insider risk means for their agency. For some agencies, insider risk occurs in the form of business fraud, while others monitor personnel risk of mental health challenges, including suicide. Improving insider risk requires collecting data and connecting the dots with other risk factors in order to develop a comprehensive picture of risk.

The Culture Challenge

Reducing insider risk involves as much people management as it does data analysis. With a workforce made up of contractors and employees hired at all GS levels, motivating a diverse workforce to identify and respond to insider threats is a real challenge. Some federal workers may be hesitant to report suspicions for fear of losing clearance or ruining a colleagues' career. Generally, the workforce is not of the security mindset and may not understand the significance of insider risk.

"Leadership is a double-edged sword."

Roundtable Participant

As such, roundtable participants suggest for agencies to consider the language used to message insider risk programs. Not only do agencies need to build trust in the effectiveness of insider risk programs, but also to assure employees that their contributions are for the overall security of the organization. By minimizing the consequences of reporting potential insider risk information, trust in the effectiveness of insider risk programs begins to crumble. Agencies must strike a balance between proactively preventing violations and avoiding wrongful accusations.

Promoting a healthy workplace culture without insider risk starts with healthy leadership. With the rise of telework and remote work, it's becoming harder to monitor employee wellbeing and their risk to the agency. Roundtable participants shared stories of disgruntled employees turning against their country, and others tragically taking their own lives. Effective insider risk programs should look outside the box to identify not only unhealthy leadership practices, but also red flags among employee communications to indicate higher risk.

Data indicates that 80% of individuals whose clearance was denied or revoked had financial or criminal issues, alcohol or drug involvement, or related to personal content. Armed with that knowledge, agencies should consider looking at early indicators of these unhealthy behaviors and thinking patterns that can lead someone down a wrong path.

But as one roundtable participant cautioned, cultural data is fundamentally different from misconduct data. If agencies are going to expand the scope of behavioral indicators to include such things as cultural or toxicity indicators, special perimeters should be formed to guide leadership on how to manage these situations. Indicators of suicidal ideation may look similar to other risk factors, and agencies should carefully consider the right person or role to investigate such risk, whether it be a manager, law enforcement, a mental health professional, or a diversity and equity expert.

Other agencies at the roundtable shared instances where an identified risk was shared with an appropriate agency to intervene, which resulted in an employee seeking help instead of committing suicide. In another instance, an agency was able to identify a group of disgruntled employees. Information was shared with another group to intervene and negative communications ceased.

Mitigating insider risk before it happens involves much more than collecting data points. An effective insider risk program shows clear benefit to the employee, and is accepted by the workforce as a standard security process. Building healthy, non-toxic leaders and creating systems to measure holistic risk are key to reducing insider risk.

To join the conversation, reach out to workinggroups@atarc.org and inquire about our newly launched **Insider Risk Working Group.**

For events on this and other topics, please see ATARC **Events calendar**.