CYBER SECURITY SUMMIT
Security solutions through collaboration.™

www.cybersecuritysummit.org

Webinar Series – May 2021

Rapporteur Report

The Confluence of Insider Threat and Cybersecurity

Cyber Security Summit Webinar Series
May 25, 2020

Speaker: Rebecca Morgan, Deputy Assistant Director, Insider Threat; Deputy Director, National Insider Threat Task Force; National Intelligence and Security Center

Moderator: Sean Costigan, Director & Co-Founder, ITL Security; Professor at George C. Marshall European Center for Security Studies

Report Author: Denna Downhour, Information Security Senior Risk Analyst, Bremer Bank; Student University of Minnesota Technological Leadership Institute – Master of Science in Security Technologies (MSST)

Speaker Bio:
Ms. Rebecca Morgan serves as the National Counterintelligence and Security Center (NCSC) Deputy Assistant Director for Insider Threat and as the Deputy Director of the National Insider Threat Task Force (NITTF). NITTF is an interagency task force co-chaired by the office of the director of the Director of National Intelligence (ODNI) and the Department of Justice. Over three decades of

Introduction:
The goal of the National Insider Threat Task Force and National Intelligence and Security Center is to provide the public and private sectors with governance and advocacy, research, outreach, and information on the latest tech developments to help organizations mitigate the risks of trusted insiders. People from all over the country and the world, from the public sector, federal agencies, and private, all have one thing in common: we all need insiders or human beings to manage and run our organizations, businesses, and missions. The following Rapporteur report outlines the discussion of the human element, or the insider threat in our organizations and information systems used to run our organizations which is the confluence of the insider threat and the cyber threat.

Insider: Any person with authorized access to an organization's personnel, facilities, information, equipment, networks, or systems.

This person can include vendors, contractors, and business partners—anyone with access within your organization.

Insider Threat: The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the organization. Insiders can cause grave harm to your organization's facilities; resources including raw materials, finished products, and information; brand, reputation, and personnel. Insider incidents account for billions of dollars annually in actual and potential damages related to trade secret theft, economic espionage, fraud, sabotage, damage to an organization's reputation, acts of workplace violence, and more.

Insider threats can cause billions of dollars in damage, including losing proprietary data, but it is so much more than this. Today, our most critical assets are information assets located on information systems, and within the cyber realm, threats to these assets happen so much faster. Recent examples include supply chain, pipeline, hospital, and school attacks. It is naïve to think that your organization will not be hit or that these attacks will not target your employees. Insiders are unique attackers as they can cause great harm, and it might take longer to identify if an adverse event has occurred. They can impact your organization through cyber means, multiplied by the ability of your employees and the access they have. The confluence of insider threat and cybersecurity causes great harm, including companies going out of business and national security incidents. This threat is looking to seek to destroy your business and steal your clients.

Cyber means typically come into play in foreign intelligence targeting, contact and recruitment. For example, social media combined with leaked information has allowed for creation of a target profile. Cultural commonalities, such as interest in the same sports team, or music, will be used in attempt to build closeness with the target. Employees going through challenging life situations such as divorce, drug or alcohol addiction, or financial troubles may post about these challenges on social media and can become susceptible to these advances.

What Makes Someone an Insider Threat?

Periods of vulnerability can cause an individual to act out and cause harm. A combination of personal predispositions, life stressors, and changes in behavior may create a period of vulnerability for an individual. When exposure is combined with a problematic response (within the home or workplace), this can cause the person to act out and cause harm.

Potential Risk Indicators (PRIs) are situations and signals that your identified person is struggling and might need help. Not everyone who displays these will go down the path and become an insider threat; it is a confluence of things that occur. However, when these indicators are noticed, they can be treated, and organizations can mitigate the risk.

Potential Risk Indicators (PRIs) Include:

- Access Attributes
- Professional Lifecycle
- Foreign Considerations
- Security and Compliance Incidents
- Technical Activity
- Criminal, Violent, or Abusive Conduct
- Financial Considerations
- Substance Abuse and Addictive Behaviors
- Judgment, Character, and Psychological Conditions

These situations and indicators can happen to anyone and be displayed by anyone. When identified, it is essential to offer understanding and assistance to ensure it does not cause more harm. To identify these indicators, we can create programs to encourage employees to speak up when they observe this behavior. Additionally, it is important that the organization manages the situation with trust and respect when information is brought forward.

Many of these risk indicators can be observed by employees, but organizations also may utilize user activity monitoring technology. User activity monitoring is a helpful tool to identify risks and is now calibrated to identify and understand risk indicators while protecting the employees' civil liberties and mitigating harm.

Risk Indicators in our Current Environment

COVID-19 has brought about a considerable shift in our cultures and how we interact with our co-workers. It has created stress, money problems, and health problems for many. These factors have coincided with sending our employees home while working on new information systems. Things we would have noticed in person we now have to try and coordinate remotely. During difficult times, there is a heightened organizational risk, and many adversaries will take advantage of targeting personal. During these times, we need greater compassion and understanding for employees and what they might be going through.

Perils and Power of Connection – Managing Insider Risk

Adversaries are good at spotting, assessing, and exploiting connection - creating perils, but there is a lot of power in the connection. Maintaining a connection with your employees goes a long way in managing risk. You know your employees and staff, and you can tell when they are having a good or bad day. You have the ability to listen and hear where people are struggling. This is the power in staying connected.

Overall, build a culture where local supervisors and managers cultivate organizational trust and relationships with employees—valuing this as a security measure beyond ensuring job satisfaction and organization quality.

Starting an Insider Threat Program

Your organization can get the basics of a program started at little to no cost. The goal is to deter, detect, and mitigate risk. A program can be created through proactive risk management by intervening and mitigating potential risks, including the following:

- Multidisciplinary Response
- Information Sharing
- Threat Analysis
- Reporting
- Privacy and Civil Liberties
- Positive Outcomes
- Training and Awareness

Conclusion

All of our organizations require insiders or human beings to manage and run our missions, while relying on technology to do so, creating threats to these assets at a rapid pace. There is no one-size-fits-all approach to starting an Insider Threat Management program at your organization; however, you can get some basics in place for little to no cost. This can start by building organizational trust and relationships with employees—valuing this as a security measure. Insider Threat Management efforts will continue to evolve and grow as your organizational needs change. These recommendations provide your organization with a proactive approach to ensure you are able to deter, detect and mitigate insider threats to your organization.