RANE Risk Assistance Network + Exchange

RANE / AIRIP Event Recap | March 19, 2018

Rising Risks in the Workplace: Managing Insider Threats

In partnership with

AIRIP
ASSOCIATION OF INTERNATIONAL RISK INTELLIGENCE PROFESSIONALS

SPEAKERS

Stephanie Douglas, Senior Managing Director, Guidepost Solutions

Dr. Marisa Randazzo, Principal and co-founder, SIGMA Threat Management Associates; Director of Threat Assessment, Georgetown University

Joel Van Heyst, Corporate Security Manager, 3M Corporate Security

MODERATOR

Rhea Siers, Executive Director, Cyber + Information, RANE

Some of the most challenging threats often "start at home" with a company's own employees, affiliates, or third-party contractors. The "insider" that can damage your physical or cybersecurity resilience may do so by accident, negligence, or malicious intent.

Not only do we need to protect against unintentional and intentional damage and attacks on our data and networks, but we need to do so in a way that delivers the right message to our workforce.

A recent RANE webinar brought together an expert panel to address the range of insider threats and provide their insights and "war stories" on anticipating, identifying, and addressing potentially damaging and destructive behaviors. Highlights of the discussion follow:

KEYS TO STARTING AN INSIDER THREAT PROGRAM

- Before you can safeguard your company's key assets against a possible internal threat, you first have to know exactly what those assets are. That means that one of the first steps to launching an insider threat program is to ***identify and catalog the most critical information***, or crown jewels, an organization possesses. As **Joel Van Heyst** put it, "You have to really figure out what you want to protect, because you can't start an insider threat program and try to protect everything. I think you need to really stay focused, and crawl before you walk."

- From the outset, an insider threat program can only succeed if it's being implemented as ***part of a broader healthy and transparent corporate culture***. "Developing a program that is respectful of employees, that has support and buy-in from the very top has to be number one," **Stephanie Douglas** noted. "Then I think it's really about good communication with your workforce. An effective insider threat program is employee sensitive, it's supportive, and still manages to take care and prioritize keeping corporate assets safe. People underestimate the importance of supporting our workforce because that's what builds loyal workers, especially if you're trying to defeat a malicious act."

- Making employees understand they all have a ***shared duty to ensure those assets are protected*** is an essential aspect of the message that must be constantly reinforced. "With intellectual property I think one thing that we've talked about, tried to communicate, is that it's actually about ***protecting your job***," **Van Heyst** said. "Because research and development is the lifeblood of our company, there is truly an incentive for us to be able to have behavior reported to us that might be concerning."

- Launching an insider threat program from scratch doesn't have to be as daunting as it sounds, according to **Dr. Marisa Randazzo**. ***"You don't have to reinvent the wheel,"*** she counseled. "If you already some type of a workplace violence program in place you can add in your cyber expertise through folks from your IT department or who have that type of technical expertise to be able to augment what the workplace team is already doing." ***Threat assessment training*** is a low cost way for your HR folks and corporate investigators to enhance their insider threat skillset.

- In much the same way, having ***strong employee conduct policies already in place*** can go a long way toward getting an insider threat program off to a good start. As **Randazzo** pointed out, "We often see insider threat happen in workplaces that lack good clear disciplinary measures and resources for poor employee behavior. When you have a case that can be handled through progressive discipline, through clear documentation, you're already ahead of the curve."

One often overlooked factor in protecting a company's valuable assets is segregating access to its systems. It's important to "have good controls in place, so you don't ever have one person with all the keys to the kingdom," Dr. Marisa Randazzo said.

IDENTIFYING (AND REPORTING) RED FLAGS

- It is important to prepare leadership on how to identify and approach red flag behavior, explained **Douglas**, as well as to assure management (and employees, for that matter) that if they voice any concerns, that this ***information will be treated discreetly***. It is essential to have in place an ***unbiased, fleshed-out investigative adjudication process*** so that leadership feels comfortable enough to speak up when a potential threat surfaces.

- "The simplest guidance we can give employees and managers," **Randazzo** stated, " is to say, 'Look, any ***behavior that starts to make you worry*** about how that person is doing, whether because you're worried about what their intentions might be, because of things that they're saying or doing, or you're worried about the possibility that they're starting to experience stress inside or outside the workplace,'" that should be reported. "I'd rather people be given a low threshold for things that may concern them, and then let the team who's trained to handle these situations look into them."

- Contrary to what many people assume, insider threats are very rarely malicious actors from the start, people who were hired without undergoing sufficient background checks and joined the company with the intention of stealing trade secrets or harming the company in some other way. The typical insider threat, **Randazzo** explained, is more often than not someone "who has been performing well or adequately for quite some time and had signed on for the right reasons" but ends up doing wrong because of some ***underlying personal problems*** (divorce, home foreclosure, debts) or failures at work.

- **Van Heyst** stressed the importance of paying close attention to an employee's ***current performance versus that of previous years***. If it seems that a very intelligent, high-performing person has suddenly become disengaged, it may well be nothing to worry about, but it could be an indication that something more troubling is going on.

- **Van Heyst** added that the ***more avenues to report malicious behavior***, the better. "That's something that we really are looking to improve at our company, especially at a place like 3M where we're so collaborative and we've got over 8,000 scientists and researchers, and well over 100,000 patents. The collaborative nature of 3M is a blessing, but it also can be a challenge because trying to determine what behavior is actually part of a person's job, and what is outside of their job, can be challenging," he said.

MONITORING BEHAVIOR AND SEGREGATING ACCESS

- When it comes to mitigating the risk of insider threats, one of the questions that companies continue to grapple with is to what degree, if at all, they should monitor their own employees' behavior or activity. "I actually find it to be most beneficial to ***not monitor unless someone has engaged in behavior that's raised some concern***, and it could be their online behavior, their system access behavior, it could be their behavior in the workplace that's offline," said **Randazzo**. At that point, depending on the particular company's policies and preferences, it may make sense to conduct some email and social media monitoring to see if they are broadcasting an intention to do harm in any fashion.

- Deciding whether or not to monitor employees on a regular basis will depend in part on your company's ***risk tolerance and past experiences*** with any insider threats, **Douglas** commented. If your organization has had previous instance(s) of malicious acts or negligent employees that caused reputational, legal or financial damage, it will likely "have a lower threshold for what you're willing to put up with."

- **Douglas** added that once a company does conclude that it needs to employ monitoring tools, it has to be very careful in how it goes about it. Many tools initially establish a baseline for an individual's behavior, so the kinds of filters that are set up will determine when a system judges that person's behavior sufficiently anomalous to warrant an alert. "What's not helpful is if you just are ***overrun with constant information because your filters are not appropriately set-up***, and you're hanging on everyone in the company."

- At the same time, it would be foolish to think that monitoring tools or system activity logs can always give you the full picture of a potential insider threat. It is critical that people making an assessment of an employee ***interpret their digital paper trail*** "in the context of everything else that's going on with that person, and the behaviors that they might be exhibiting that don't touch the digital realm," as **Van Heyst** noted. No matter how sophisticated, no technical solution is going to render a clean, guilty or not guilty verdict; every tool requires ***"the human element,"*** as moderator **Rhea Siers** pointed out, to interpret "what your technology is telling you."

- One frequently overlooked factor in protecting a company's most valuable assets, especially with fast-growing startups, is segregating access to a firm's systems and trade secrets. "Making sure that people have access to ***what they really need to have access to***, that there are rules and procedures around how they protect that information, is critically important," said **Douglas**. Those rules should include not just who has access to what, but also if and how such things as laptops, thumb drives and cloud services should be used remotely.

- **Randazzo** echoed that point, recounting how she has often encountered insider threat cases in which a system administrator enjoyed virtually unlimited access while being supervised by someone with a nontechnical background. "One thing that can benefit companies is having ***good controls in place***, so you don't ever have one person who has all the keys to the kingdom."

> ***"it is easy to put insider threat into a box, whether it's a cybersecurity function or a corporate security function...but it will not work if it's siloed off in one specific area of the company."***
>
> ***- Stephanie Douglas***

THE IMPORTANCE OF A MULTI-DISCIPLINARY MANAGEMENT TEAM

- Just as every employee at a company has a job to do (of looking out for and reporting a colleague's troubling behavior) in an insider threat program, the program itself must include a ***wide range of functions at the top*** for it to succeed. **Van Heyst** noted that 3M has done just that, pulling together a cross-functional team, modeled after its workplace violence prevention group, to assist in evaluating high priority cases, identifying risk tolerance, retrieving technical advice from IT and intellectual property experts, and determining next steps.

- **Douglas** also stressed the importance of a cross-functional team, saying "it is easy to put insider threat into a box, whether it's a cybersecurity function or a corporate security function…but it will ***not work if it's siloed off in one specific area of the company.***" In addition to the more obvious departments such as IT and physical security that need to be at the table, decision-makers from HR, Employee Assistance Programs (EAP), legal, compliance and the business side also should be involved.

- Two critical benefits of this approach, according to **Randazzo**, are that "when you've got all those areas represented, you're more likely to hear about whatever the problem is earlier on, and you're actually able to gather information more readily because you have people already positioned in these silos." Most important, she added, a multi-disciplinary team allows for ***more informed and proactive decision making*** to take place. "Together the team can say, 'What can we do, A. To support the person, but B. To keep the workplace safe? What can we do from a cyber angle? We can monitor or lock out all of their access. Going from a physical angle, we can provide additional security or move co-workers around who aren't feeling safe? What can we do to support the employee, we've got EAP. We've got supervision. We can transfer within the company."

- **Randazzo** went on to explain how just having ***only one supervisor or department*** make the call on an employee exhibiting troubling behavior, "without looking at the big picture," can actually increase risk. Simply terminating a person without involving physical or cybersecurity teams and failing to cut off access to facilities, people, systems and trade secrets, for instance, can expose an organization to greater physical or virtual danger. On the other hand, leaving such a critical decision up to a single individual can mean that potential insider threats aren't rooted out early enough. When Randazzo was at the Secret Service, she researched an incident in which a high performing stock trader at a financial institution began to drink and take prescription drugs on the job. Co-workers reported his erratic behavior but were told by management, "Don't bother him. He performs so much and brings us so much in terms of revenue and profit. We're just going to leave him alone because he's still performing." On a separate occasion, the IT department reported to the same supervisor that the employee in question was accessing trading in foreign markets after hours, which went against the organization's rules. Yet again nothing was done about the situation and, as a result, the company eventually lost hundreds of millions.

> ***"You have to really figure out what you want to protect, because you can't start an insider threat program and try to protect everything."***
>
> ***- Joel Van Heyst***

ABOUT THE SPEAKERS

Stephanie Douglas, Managing Director, Guidepost Solutions
As a Senior Managing Director in the San Francisco office of Guidepost Solutions, Stephanie Douglas focuses on compliance, sensitive internal investigations, white-collar crime investigations, and workplace investigations and develops holistic corporate security programs. She works to provide executive education and training in a number of areas including crisis management and insider threats. Douglas is highly respected in both private and public sectors. She retired as a Senior Executive from the Federal Bureau of Investigation in 2013 after serving in a variety of roles over 23 years, including Executive Assistant Director of the National Security Branch ("NSB"), Chief Intelligence Officer, and the Special Agent in Charge for the FBI's San Francisco Division. After her tenure at the FBI, she joined Pacific Gas & Electric, as its Senior Director of Corporate Security, overseeing risk mitigation and issue response.

Dr. Marisa Randazzo, Principal and Co-Founder, SIGMA Threat Management Associates LLC; Director of Threat Assessment, Georgetown University
Dr. Marisa R. Randazzo is a national expert on threat assessment and targeted violence. Before joining the private sector, Dr. Randazzo served for ten years with the U.S. Secret Service as the agency's Chief Research Psychologist. She directed all Secret Service research on school shootings, insider threats, stalking, and other types of targeted violence. Dr. Randazzo is an accomplished presenter and instructor on threat assessment investigations, having trained over 10,000 law enforcement, intelligence, and security professionals throughout the United States, Canada, and the European Union. Her research is used in the federal, state, and local law enforcement communities and has been credited in the media with preventing planned attacks. Dr. Randazzo previously served as a Senior Expert with Business Intelligence Advisors, Inc., where she provided high net worth families, corporations, and schools with investigative consultation on individual threat cases and training on threat assessment, bomb threat assessment, and the detection of deception.

Joel Van Heyst Corporate Security Manager, 3M Corporate Security
Joel Van Heyst started his professional career in health care with the Department of Veterans Affairs. A transition to the Federal Bureau of Investigation led to assignments investigating white-collar crime as a Special Agent in Minneapolis and Chicago. In 2007, Van Heyst joined 3M as a Corporate Security Manager supporting a variety of business groups, investigating allegations of employee misconduct and workplace violence, and reviewing physical security at 3M facilities. He now manages the Risk Mitigation team supporting the United States and investigates insider threat cases.

ABOUT AIRIP

The Association of International Risk Intelligence Professionals (AIRIP) is a nonprofit business association for risk intelligence analysts and those interested in the profession. AIRIP focuses on, but is not limited to, the areas of business opportunity, physical security, cybersecurity, reputation and political risk intelligence. Learn more at www.airip.org

ABOUT RANE

RANE (Risk Assistance Network + Exchange) is an information and advisory services company that connects business leaders to critical risk insights and expertise, enabling risk and security professionals to more efficiently address their most pressing challenges and drive better risk management outcomes. RANE clients receive access to a global network of credentialed risk experts, curated network intelligence, risk news monitoring, in-house analysts and subject matter experts, and collaborative knowledge-sharing events.