Insider Threat and Workplace Violence

featuring Carrie Gardner and Tracy Cassidy as Interviewed by Eileen Wrubel

---

Eileen Wrubel: Welcome to the SEI Podcast Series, a production of the Carnegie Mellon University Software Engineering Institute. The SEI is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University. A transcript of today's podcast will be available on the SEI website at sei.cmu.edu/podcasts.

My name is Eileen Wrubel, and I am a tech lead for the SEI's Agile-in-Government Practice. Joining me today are Tracy Cassidy and Carrie Gardner who are both researchers in the CERT Division's National Insider Threat Center. Today, we are here to talk about their work on workplace violence and insider threat.

Let's start by having you each briefly talk a little bit about your background and your experiences, how you wound up at the SEI, and how you wound up doing work on insider threat.

Tracy Cassidy: I was working as a psychotherapist in California for a long time, and so I have a psychology background. I worked with the U.S. Department of Justice's U.S. Pre-Trial and Probation Services and Federal Bureau of Prisons. I did therapy and assessments with clients going in or coming out of prisons. A lot of them had committed insider threat acts, so I have familiarity with working with clients who have done that kind of crime. Also I am interested in the human elements behind cybersecurity. So that is what led me here.

Eileen: OK, and Carrie?

Carrie Gardner: I celebrate my one-year, full-time anniversary in June. Before that though, like Tracy I have more of a non-traditional background. As an undergraduate, I studied the social sciences focusing on political science, psychology, and criminal justice, gearing myself for an intel-analysis position. Then when I had an internship there I was focused on cyber, so I decided to pursue a technical master's degree in information science, which brought me here to Pittsburgh where I got an internship at the SEI on the Insider Threat Team. So I am able to use those knowledge, skills, and abilities in the insider threat domain, which is a very multidisciplinary space. I really enjoy that.

Eileen: For our audience members who don't know a lot about this area of research, could you talk briefly about what we mean when we talk about insider threat? What does that really encompass?

Tracy: The CERT National Insider Threat Center has been working on issues of insider threat for the past 16 years. Several of the people on our team were the ones who pioneered that work. The focus has evolved from looking more at technically detectable insider threats and now involves more of the behavioral aspects.

When we are talking about insider threat, we are talking about individuals who have or had authorized access to an organization to use their assets either maliciously or unintentionally to act in a way that negatively impacts the organization.

Things like theft of intellectual property, sabotage of IT systems, national security espionage, fraud, particularly in the banking and finance sector and healthcare sectors, and terrorism. We also look at unintentional insider threats. So those have to do with things like clicking on phishing emails or leaving your work laptop at the bus stop.

Because of the evolution of insider threats, we are also looking at terrorism and workplace violence, so more on the behavioral aspects. We are focusing on workplace violence and insider threat, or harm of self or others, because a lot of times people who are on the pathway to violence are also suicidal but not necessarily vice versa. So that's why we're looking at both of them. Also, DoD and federal government spaces are mandated to set up insider threat programs, and they are also mandated to involve workplace violence in those.

Eileen: Can you tell me a little bit about your research process and your research objectives for this work?

Carrie: We started with a literature review and assessed the psychology and criminal justice literature that studied workplace violence. And then even the social and information sciences, to see where workplace violence is going in the field. And then we also did some case coding. So we collected workplace violence incidents and coded the incidents on fields that we thought were relevant for insider threat research. From there we were able to then create a factor-tree model of all these different variables associated with the incidents and categorize them into different groupings. A chronology naturally fell out that gave a temporal description of how a particular incident unfolded. So we can see precursor events that foreshadowed the event or the escalation of events that were to occur. After that factor tree and in the chronology that came from it, we are able to then pull out indicators, which take observables preceding the event, and then we can identify controls or safeguards that can be used to measure those indicators.

Eileen: And what kinds of indicators would we be talking about, just a couple of examples?

Carrie: On the behavioral side, perhaps anger, HR [human resources] formal policy violations or technical violations even. Or if there's someone who is visiting dark websites, that could be something of concern.

Eileen: So can you tell me about your research objectives?

Tracy: In thinking about the technical detection of insider threat, we realized that there were not a lot of known capabilities for insider threat tools to understand a heightened risk of workplace violence. We realize now that this ability is augmented by new cyber data that is available through HR records and personnel records. They can give us some more information about behavioral pieces of insider threat.

Our solution was in support of the DoD and mandated insider threat programs in their efforts seeking to discover technical and sociotechnical indicators, which can be used in operational environments to strengthen the capabilities of these tools. Basically our end game is to look at how to mitigate the risk these employees may pose to themselves or others within the organization.

Eileen: So how did it go? What were the findings or the artifacts that you were able to produce?

Carrie: We have three main findings. The first was a development of the chronology, which takes previous work and the pathway, the critical pathway from Eric Shaw and our work at the National Insider Threat Center.

The second was indicators and controls. So how can organizations put into place operational controls to measure indicators of workplace violence? And the third was, this really is a strong exemplar of the need and value-add of incorporating behavioral data into an insider threat mitigation strategy. I think that is a big one across the insider threat domain as a whole.

Tracy: As far as the artifacts, as Carrie said, we have the pathway to intended harm that we developed, which was based on the critical pathway from our work with Eric Shaw years ago and also a combination with the pathway to violence by Calhoun and Weston. And so we married those two together and also morphed it into one that will look at issues of intended harm to self as well as to others. And we call that the "pathway of intended harm." We also have the blog post, Workplace Violence: An Insider Threat. We will be releasing a white paper soon and a full report. We are expecting these hopefully by the end of the summer, and we are presenting at several conferences on the topic coming up.

Eileen: I am glad to hear that. So I am not familiar with a lot of this terminology. I am wondering if you could give me and our viewers a description of what that pathway toward intended violence looks like.

Tracy: The start of our pathway has personal predispositions. So, *What is happening for the person in their life that might push them more toward going down a pathway?* Things like that can be family history of suicide or substance use in the past. [Additional Information: If the person is facing life stressors whether from workplace and professional issues or personal stressors, such as illness or relationship or financial difficulties, they may be at an increased risk to act out in ways that we call *concerning behaviors*]. When people start moving down the pathway to concerning behaviors such as conflicts in the office, missing work, absenteeism, things like that, when those two things come together and they start moving toward being disgruntled or getting further into depression from feeling suicidal, they move into a, *I could do something to stop this situation*, whether it be hurt to someone else, hurt themselves, or both. And then they move into the, *I would do this. I am going to move forward and I am going to…*, it is kind of their tipping point and they move forward. Maybe something at work happens where they don't feel organizational support. So they are looking at what they call probing and breaching. They are looking at checking out the work environment and seeing maybe where they could come in and do something, watching people's schedules, things like that, and making plans to move forward. There is also a lot of leakage behavior that happens around that time where people are actually telling people that they are wanting to do this.

In a fair number of cases they actually do tell someone, which is an ability for the technical detection to pick that up if they're doing it via email. Or telling a co-worker to stay home from work so that they are not showing up on the day that the rampage might happen. And then if it doesn't stop at any point along this path, they can move forward to the violent act itself.

Eileen: Thank you for walking me through that.

Carrie: To go along with what Tracy said, one of the things that we are looking at is operationalizing these threat scenarios—taking model examples of workplace-violence incidents and creating scenarios where we can simulate this activity in our test environment.

At the National Insider Threat Center, we have a tool-testing lab where we take industry tools, and we can test and validate these tools that they can see observables of insider threat activity, to see if these controls in the measuring process are able to detect and prevent those activities from occurring. We can then take these scenarios and simulate the activity into scripts, and the next process for this work plan will be taking that and validating and simulating the activity in the tool-testing lab.

Eileen: So you talked a little bit about this, but what's next? Where do you see this headed in the future?

Carrie: I think like the big next thing is, number one, case coding more incidents. So just collecting more data, gaining more insight into the models and what we can extract from those.

Then, for me, I definitely want to incorporate some text analysis. One of the things I focus on at the SEI is to do natural language processing and seeing if we can detect observables early on for prevention. An example for this would be, can we have some kind of capability where we read employee emails and then identify that anger, for instance, was spiking? And can we stage an early intervention perhaps with that?

So it's an intervention mitigation strategy for that. And then again, going back to the scenarios and simulating that threat activity and then evaluating if those tools for insider threat mitigation can apply to these type of incidents where we can observe and then measure and perhaps even detect when precursors or indicators of workplace violence are actually taking place.

Eileen: Do you have anything to add Tracy?

Tracy: In our group we work on helping people build their insider threat programs and so it is really important, as they are thinking about workplace violence, to pull from their threat-assessment teams and work together to have a more full picture of who the person is because that is the most important thing—to understand the employee holistically.

And also in addition to looking at building insider threat teams, I think that it would be really important to look at the workplace-violence work that we have done and combine it with the positive incentives work that we have done, which we have a podcast and blogs on as well, and look at how we can help people along the way. What positive incentives can corporations implement to help people before they move further down the path? And also in thinking about future work, it would be great to try to replicate the work that we did with this project in looking at pathway to radicalization because that is definitely another national security issue that is going to be coming up in the future.

Carrie: And then to build on what Tracy said, it would also be interesting if we could acquire some label data sets of user log activity for instance, and seeing if we can then extract information or precursors before the escalation event occurred. So we can perhaps gain information on what they were doing technically, or perhaps who were they chatting with, what websites where they were visiting, before the actual incident. And that would really interesting.

Eileen: Well, thank you both so much for joining me today to talk about this. Tracy has also offered a blog post on *Workplace Violence and Insider Threat* that can be found at insights.sei.cmu.edu. Click on the author tab and find Tracy Cassidy's name. That's Cassidy with a C. We will also provide links to the resources mentioned in this podcast in the transcript.

This podcast is available on the SEI website at sei.cmu.edu/podcasts and on Carnegie Mellon University's iTunes U site and the SEI's YouTube channel. As always if you have any questions or want to discuss this further with us you can reach us at info@sei.cmu.edu. Thank you.