Positive Incentives for Reducing Insider Threat

featuring Andrew Moore and Dan Bauer as Interviewed by Will Hayes

----

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

My name is Will Hayes. I am principal engineer here at the Software Engineering Institute. It is my pleasure to introduce two of my colleagues, Andy Moore and Dan Bauer. If we could start by having the two of you each explain a little bit about who you are, where you come from?

Andy Moore: Thanks, Will. I started my career at the Naval Research Lab working in the area of formal methods applied to cybersecurity. In 2000, I came to the SEI and started working for the CERT program, so, it is still cybersecurity. Shortly thereafter, I started working in the insider threat area, which I felt was kind of a new security area because it is, basically, a people problem. So, it combined the technical work that I like to do with some very fascinating people problems.

Will: And Dan?

Dan Bauer: Sure. I have been with the SEI a little more than two years, now. I have spent the last 20 years working in the human resources/talent management field. Here at the SEI, my team focuses primarily on day-to-day employee-relations types of activities, but we do engage with leadership from time-to-time at a strategic level. And this particular research that Andy was fortunate enough to introduce to me lends itself pretty handily to a lot of the current and emerging talent management practices that look into employee/employer relationships.

Will: We have kind of a unique internal collaboration going here where we have got a line of very successful and well-known technical work. And not necessarily an internal laboratory, but we've got professionals who are part of the audience for this kind of work. It is kind of cool that we have had a chance to do this internally.

Andy: I am glad you noticed this. This is really the exciting part of work, this collaboration that we have got going here.

Will: One of the things I read from the prep for this activity, that in 2016 Cybersecurity Intelligence Index, IBM found that some 60 percent of all cyber attacks relate to insiders. Could you talk a little bit about that prevalence?

Andy: Yes. So, the insider threat problem has continued to be a rather hard problem. It has become worse over the years actually. You go back a few years, and it was almost all about external threats: people on the outside, external to an organization, getting in. It is still a problem, but as the defenses for organizations get better and better, *what is the avenue in*? It is harder and harder to get through their boundary defenses. So, *what do you do*? Well, you look for that insider. The insider is an employee within an organization that has authorized access already. They are in there, and if you can get them to do what you need to do, from the adversary's perspective, then that is the easiest route in. So that is becoming more prevalent.

In addition, the nature of the insider threat has changed over the years. You go back a number of years, and is was mostly about financial means, making money, especially when there's financial stresses, personal stresses in the family. You might use your access in order to make ends meet so to speak.

More recently, it has become a lot more ideological. Especially [insider threat] goes back and forth with the economy. As the economy is worse, people get into financial problems, and the financial crimes become more prevalent. Recently, it has become a lot more ideological.

The focus in the insider threat research community has been primarily looking at the person, what they did wrong, and how you can detect increased risk of what the person is doing. Our approach is to not only look at that but also look at organizational behaviors that can be conducive to the insider threat.

In particular, we are focusing in our initial work on something called perceived organizational support. So, this is how well the organization is supporting the workforce. If this is not high enough, what we see is insider threat attacks go higher. Organizational behaviors can directly influence the rates of insider threat. If you let those persist, what happens? Those same threats are going to recur as a natural consequence of those practices.

Will: This is really a natural place to turn to Dan and talk about positive incentives and how they play into this. Could I ask you to comment on that?

Dan: To build on what Andy said that beyond just the personal or the individual perspective and more on the organizational perspective, it is actually not all that surprising that when the

relationship between the employee and employer changes or is at least perceived to change, there is a negative outcome to that. As a result, it can be rather unpleasant. For instance, if an employee perceives that the support that they are receiving from the organization in areas like compensation, recognition, rewards, communication, professional development, and things like employee systems, they do not feel that is adequate as a whole, then all sorts of things start to happen from a behavioral standpoint. As a result of that, there can be job dissatisfaction, retention issues, other sorts of professional issues, and unfortunately even insider threat.

Will: So the notion of a disgruntled employee taking that energy toward something that is really detrimental to the mission of the organization, what you are talking about really is to prevent that situation from arising, to prevent that sentiment from being the driver. So tell us a bit about your research on that.

Andy: What we are looking at is a group of workforce management practices, which we are calling positive incentives. As I mentioned, perceived organizational support is a category of positive incentive. Others involve job engagement, connectedness with co-workers. So, really, there are three dimensions to the problem: job, organization, and people.

We look at these positive incentives and say, *Hey, these can help naturally align employees to the organization's goals*. So, as a natural consequence of those incentives, they are acting in the interest of the organization.

This contrasts with kind of a traditional security approach, which is instead of attracting people to act in the interest, they are attempting to force people. So, this is policy constraints, technical constraints, detection of misbehaviors, and punishment of those misbehaviors. We call those negative incentives.

Now, we are not saying the positive incentives, which attract people in, replace negative incentives. But we are saying a combination is needed. The community has really almost solely focused on these traditional practices, which are negative incentives.

So, the positive incentives, by their nature, focus more on the organizational behaviors, as opposed to employee behaviors. Now, what do I mean by *organizational behaviors*? Well, we are really looking at workforce management practices and how those are applied by the managers within the organization.

Will: So, it seems that—let me address perhaps to Dan this question—that if we continually focus exclusively on the negative, we are in a race. We are really trying to stay ahead of the really capable people we want to hire in our organization because we think that their energies are going to be applied to something negative, something that is opposed to the organization's mission. A person in a role like you have really has an obligation to create a professional

working environment. That is not a race. That is a foundation in which the race becomes less important. Is that a fair way to say it?

Dan: I think that is accurate. To mirror what Andy said, certainly a combination of both is the key. From my perspective and from a human resource perspective, you would love to see the positive all the time, but even in those types of instances it is not always possible. So, trying to find that right balance between a constructive and supportive approach that the organization presents and management presents is way more appealing and interesting to employees than one that is perceived as punitive or distrusting.

Will: So, there is a certain sense of, *Create the environment in which people can pursue their chosen profession to an excellence*. That is the obligation the organization has, not just run the race of trying to make sure people stay in their box.

Dan: Exactly.

Will: Maybe I will address my next question to Dan. One of the things about the Software Engineering Institute is that we are transition agents for ideas and capabilities like this. If I am one of your professional counterparts out there working in a different organization, how do I pursue learning about this?

Dan: Sure. When I first learned about this from Andy, what really got me excited about engaging with his team was the potential implications to human resources and talent management. Obviously, the initial focus was on the insider threat side of things, but I find it very, very appealing in terms of what we are trying to do. Quite simply, engaging with employees in ways that they perceive as providing support can improve employee satisfaction, performance, and retention. This includes focusing on valuing their contributions, caring about their well-being, and also supporting their socio-emotional needs and treating them fairly.

I realize this might sound like common sense, but unfortunately it is not something that always happens in organizations. Many organizations get caught up in the day-to-day operations, and they do not necessarily have the time and energy to focus on these sorts of relationships. Nonetheless, it is important to make sure that you do focus on them.

Really the big takeaway in this piece from the HR perspective is that leaders and other HR folks should be focused on incorporating positive measures within their workforce management practices. From my perspective, enabling employees to be more satisfied, productive, and compelled to stay with an organization should be a goal for all organizations, quite frankly. Especially since this approach can pay dividends, as you discussed earlier, not just with your current staff, but also attracting new staff to come and help with the projects and the work that we need to complete.

Andy: That is a good point, Dan. If I might add as well, I think the benefit of these positive incentives is not only the things that Dan talked about with regard to retention, improved performance, and satisfaction, but from the insider threat perspective, if it is worth a comment there, too. What we have seen with insider threat is there really needs to be this close collaboration between human resources, insider threat researchers, information technology, and other departments within an organization like security and legal and privacy, as well.

What we tend to say is that what we are looking for is, *What is the balanced combination of these positive incentives with the traditional practices?* If you focus too much on the traditional practices, where they are negative-incentive based, you end up with a Big Brother program. The guy is looking over your shoulder and making sure you do not do bad things. We think with this good-balance combination, you can really get a good employer program that is in there, making sure that people are behaving consistent with the organization, that you attract people into that. Of course, there is always the potential for somebody to act out and go down that bad path. That is why you really need the combination of positive and negative incentives.

Will: This conversation reminds me a bit of some work by a guy named Dan Pink, who has done some really neat stuff that kind of substantiates that autonomy, mastery, and purpose are things that people pursue. It sounds like you want to foster an environment where autonomy, mastery, and purpose are valued. The big brother picture is not really commensurate with that.

Andy: Yes. I think Dan talked a lot about engagement. I think those sorts of things are critical to employee engagement as well as motivation and so forth. You hit the nail on the head with regard to looking at issues. *How you motivate people in the right way*? There is a lot of literature out there that our work builds upon.

Will: Great. So, you spoke of collaborators a moment ago. I have seen a report where you had a pretty diverse cast of authors in there. One of the marvelous things about being at Carnegie Mellon is we get to collaborate with some great minds. Could you talk a bit about the net you were able to cast here?

Andy: That is my favorite part of working here is the collaboration that we can do. Because we can work with campus, and we can work with other departments within the SEI. Our campus work here was with professor Denise Rousseau. She is with the Heinz School at CMU and also at the Tepper School of Business. She is an organizational psychologist. And years ago, she developed a notion called ''the psychological contract.'' This is an implicit contract that all employees have with their organization. It is not written down, usually. But interestingly, our insider threat research found that it was essentially a breach of the psychological contract that caused employees to commit these cyber misbehaviors.

So, that has been great. Because she has been able to direct us, inform us about the background literature and keep us on track with how to help organizations.

The work I have done with Dan, as I mentioned, and his talent management team—we had three people from his team working with us on this—really is a milestone in my career getting to work with them. They bring a credibility and a grounding for both our research and our applications, and, in the future, some piloting with organizations we hope.

Will: Great. It sounds like you've got a combination that takes the concepts and the theories and makes them much more practical, much more applicable. Because we have taken it to engage people that are doing things, day to day.

Andy: Exactly. We went in with an idea from the theoretical perspective, and Dan's team really helped us refine that down into saying, *Well, these things really do not* work, or *These other things we should think about and add into our taxonomy of practices*.

Will: This notion of a psychological contract is a really intriguing one and it really makes a lot of intuitive sense. It would seem to me that there are HR practices that stem from the recognition that such an underlying phenomenon really drives what is going on. As we think about the influence of the negative practices, the attempts to control and prevent, it would seem that many of the organizations we serve, particularly in the government, have people who are in a position to be at the head of these kinds of things, that are ahead of us in knowledge on these areas. The amount of space available with the negative controlling approach is diminishing I think over time. Would you comment on that?

Andy: Yes. I think that is right. We have had a number of organizations come to us and basically say that they are required to put in place these insider threat programs. Since they are based in these traditional security practices, often they are negative incentives. They are constraints. They are monitoring employees. There has been some push back, I think, by employees on the negative slant to these practices. The hope here is really that as organizations look at more of the organizational behaviors that might be conducive of the threat that, as you put in place these positive incentives, it creates an insider threat program that is more of an advocate for the workforce as opposed to detect and punish.

Will: That really speaks to what you do doesn't it?

Dan: It does. To add to what Andy said, when I think of that component of the positive and the negative, I think of performance management, which is a pretty significant function within HR/talent management. Not surprising, a lot of the research and practice focuses in more on balancing that.

It is a tough conversation. No one wants to sit across the table from their supervisor and hear all negative things. So, blending that, that is the sort of thing that happens in performance management with the goal of we seek to drive behavior in the correct direction. But it's more obviously appealing as we discussed before.

We often use the term the *performance feedback sandwich*, where the bread is the positive, and the meat is the negative. Start at the top, bread. You start off the conversation being very positive. The meat is the negative where you have to tackle the challenges of areas for improvement. You finish up again with the bottom part of the bread there, with the positive takeaway for the employee. I think it is a very similar approach in the way that we handle performance management and can lend itself well to insider threat.

Will: Where is this going? What is in the future for you? What's next?

Andy: I think, from the research side, there's a number of interesting aspects that we want to go down. One is tools. You might ask, *well, this is very behavioral, social…*

Will: People oriented.

Andy: *People oriented. How can tools help*? Well, you might think, *well, the first idea might be that, well, why not existing HR kind of employee performance management tools*? They very well could be helpful.

One class of tools that is just kind of emerging is something called employee relationship management tools. So, this, you probably have heard of customer relationship management. So, that has been around for a long time. And it is a similar idea.

But this is direct relationship between the employee and the organization. And in fact, the best use of these for working in the positive incentives is applying the tools for a supervisor and the relationship of that supervisor with the direct reports. These kinds of tools can actually help ensure that as problems arise, issues are dealt with positively and that the supervisor has access to a range of positive incentives that they can apply in different situations.

Will: One of the things that we emphasize in some training that I deliver is engagement is a really high priority. It would seem that an avenue through a communication channel like a tool might be a way to assure or even perhaps gauge the level of engagement. Is that a feature you are seeing?

Andy: I think that that is a good point. I think engagement is especially critical, especially when you have that perceived organizational support foundation. Building upon that with engagement is going to deliver a lot of the benefits that Dan has talked about in terms of satisfaction and performance.

Dan: Engagement actually is one of the areas. It is really hot in the field in talent management, but I also have been very interested in it myself. The timing of engaging with Andy on this is huge because I had already been looking at some surveys that I want to try to utilize within our own organization to tap into engagement. Because I agree that finding a way to measure that and look at that and understand it within organizations is critical.

I also think—to build on what Andy was saying with the tools—that there are some systems that are out there and more that are being developed that help address those sorts of things. More importantly, we talked a little while ago about organization supervisors not having the time and the energy. Well, this helps fill that gap. If there is some technology that can be utilized to give them more time and to do it in a streamlined fashion and to build that organizational support, why not utilize the technology to do that?

Will: It can aid in continuity of conversations that have to happen on a periodic basis. It can be much more of a smooth flow of communication.

Dan: Exactly. Another component of this—there is the tools, there is the engagement—but I also look at the cultural piece. *How do organizations handle that?* From that perspective, there's no easy answer to that question. Culture cannot be fixed overnight. There is a lot of communication, support from leadership to build in these tools, these practices to make them effective. We do not give up. We keep plugging along and do what we can, at least from an HR standpoint, to make sure that we do not lose focus.

Will: If I might make an observation, it would seem that your ability to participate in this is a positive incentive for you as an employee in the HR Department, that a meaningful addition to what you do can be found through this kind of research.

Dan: Absolutely. Because I do like to keep tabs on my field, but that involves benchmarking and looking outward at other organizations and other research that I find. Actually to be involved directly with the research, with someone like Andy and his team, has been an incredible opportunity for me. To realize that not only from the research perspective, but then, ultimately—especially as we engage further with Denise—looking at best practices and other ways that we can take this to help organizations with this issue.

Will: The positive incentives for Andy are to have more opportunities like this, and to work with other scientists in the field, and other organizations trying out and learning from the model that you are representing.

Andy: It is really fascinating work. And I find that the collaboration we get is the most meaningful part of the work, really.

Will Hayes: Really cool stuff. Thanks very much, for your time, today. I appreciate your joining us.

Andy: Thanks a lot, Will.

Dan: Thank you. It was great.

Will: Thank you for joining us, today. This podcast is available on the SEI's website at sei.cmu.edu/podcasts, along with a transcript. This podcast is also available on SEI's YouTube site, as well as on Carnegie Mellon University's iTunes U site. As always, if you have any questions, please don't hesitate to email us at info@sei.cmu.edu. Thank you.