Shane McGraw: Hello and welcome to today's SEI webcast, balanced approaches to insider risk management. My name is Shane McGraw, outreach team lead here at the Software Engineering Institute, and I'd like to thank you for attending. We want to make our discussion as interactive as possible today, so we will take questions throughout today's talk and you can submit those questions in our YouTube chat area, and we will get to as many as we can. Our featured speakers today are Randy Trzeciak and Dan Costa. Randy is our director of the CERT insider risk management team. He's also director of the master of science in information security policy and management program in the Heinz College at Carnegie Mellon University. Dan is the technical manager of the CERT insider risk management team. He's also a certified information systems security professional and IEEE professional software engineering master and an adjunct professor in Heinz College at Carnegie Mellon University. Now I'd like to turn it over to Randy Trzeciak. Randy, good afternoon. All yours.

Randy Trzeciak: Thank you, Shane. It's a pleasure to be with you here today from the campus of Carnegie Mellon University. It's a privilege to be here working alongside of Dan Costa and sharing some of the thoughts and ideas around insider risk management and the research that's actually happening here on the campus of Carnegie Mellon University. Just as a bit of background, a bit of a history of the work, where we've come from and where we're currently at today. If you're not aware, we're part of the Software Engineering Institute, which is the federally-funded research and development center housed here on the campus of Carnegie Mellon University. And as a federally-funded research and development center, our mission is to do research in two primary areas: software security as well as cybersecurity. Now within the context of the cybersecurity research areas, the focus on insider risk and insider threat identification, and insider threat mitigation. So it's a pleasure to be here and we're coming to you from one of the six directorates, which is the cyber risk and resilience directorate in the CERT division of the Software Engineering Institute. So it's a pleasure to be here, and we hope over the course of the next few minutes we share some thoughts and ideas around the research that's happening, but also take your questions. So we strongly want to encourage you to put your questions in chat. Happy to answer those throughout our session today.

So I'd like to, again, introduce Dan Costa. So Dan, what I'd like to do is maybe kick this off by recognizing National Insider Threat Awareness Month, and then specifically looking forward to the contributions that you and your team are doing in relation to the insider risk symposium that's coming up. So if you wouldn't mind, maybe give us a brief preview of what to expect later on in the month, please.

Dan Costa: Yeah, certainly, Randy. Happy National Insider Threat Awareness Month. And this is the third year, I believe, here in the States at least, September has been recognized as National Insider Threat Awareness Month. This year we're proud to be hosting our eighth annual symposium on insider threat mitigation, and insider risk management. This year, we're calling it the CERT insider risk management symposium. So this year, we'll be hosting the event over the course of two days, September 28th, September 29th. It will be from 11 AM to 1 PM Eastern both days, and we've got a really exciting slate of presentations and panelists, panel discussions set up. The theme this year is balanced approaches to insider risk management, and one of the things that we'll do hopefully, during this webcast, is unpack that a little bit.

One of the other themes that you'll find from us this year is an emphasis on highlighting a lot of the research that we've been doing here at CMU over the past year. We're excited to be releasing several new technical reports, an updated version of our common sense guide to managing insider risk, as well as a variety of other publications that we've put out, and other measurement tools that we've been putting out over the past year, or hope to have out between now and September 28th, September 29th. So really looking forward to taking advantage of just sharing with the community all the great work that the team's been doing over the past year, trying to find ways to connect folks to those resources, help them understand what we've put together, how we went about putting it together, and how they can use it to help their organizations more effectively manage insider risks.

So we'll start things off on the 28th with some opening remarks from the CERT division director, Greg Touhill. You'll kick things off, Randy, and then we'll roll right into our first presentation, which will be Carrie Gardner, our insider risk team lead, and myself, providing the community with some updates on things that are new from us by way of publications, presentations, other places you can catch us talking and getting our research out, not only in National Insider Threat

Awareness Month in September, but also in October, when we roll right into Cybersecurity Awareness Month. So September and October are busy times here within CERT.

After that conversation, we'll have our first panel, where we'll be talking about emerging trends and technical approaches to insider risk quantification. So I'll be leading a conversation with a lot of our fantastic engineers that are out helping insider risk management programs align their technical detection capabilities with the changing threat landscape, as well as taking the bits and bytes that come off of our technical detective capabilities and aligning those to how organizations make risk-based decisions at the enterprise level. So that'll be our first day.

On day two, we'll start things off with a presentation from Brett Tucker, our cyber risk management technical manager here, within the cyber risk and resilience directorate, where Brett will be talking to us about the relationship between insider threat program operations in that broader enterprise risk management function, using ransomware controls as examples-- as an example by which we can walk through how insider threat program practitioners, how insider threat controls, can inform risk-based decisions that happen at the enterprise level, with regards to how well-prepared the organization is to deal with things like ransomware, and the human elements that are associated with protecting our organizations against ransomware attacks.

After that presentation, we'll wrap up day two with another panel, this time from our researchers in insider risk, where we'll be talking about balanced approaches to insider risk management. So how do we augment and supplement our technical detection capabilities with administrative and management controls, things we might not necessarily traditionally think about when we're thinking about security controls, to increase the levers of perceived organizational support, organizational fairness and connectedness at work, which our research has demonstrated have positive co-relationships between those conditions and organizations' kind of security postures that pertains to insider threats. So how do we narrate the technical and the behavioral approaches to writing balanced insider risk management capabilities within our enterprise. So two really great panels from both our research teams and engineering teams here, as well as some special topic presentations and really, the goal of these will be to be as interactive as possible. So for both those panel sessions, for the what's new presentation, and for Brett

Tucker's presentation, we'll have Q&A sessions on the back end, giving the audience a chance to engage with our researchers and our engineers.

So that is a 50,000 foot overview of what to expect and we certainly hope everybody watching this webcast will join us on the 28th and 29th.

Randy Trzeciak: Well, thanks, Dan. That certainly gives a nice highlighter preview of what's to come later on this month. Now if we look back to the years of research, the insider threat body of work really started here in CERT around the year 2001. So we're over the 20 year mark, focusing on insider threat identification and insider risk perspectives around insider threat mitigation as well. And over the course of that time, what we've tried to do is build that empirical knowledge, you know, basing the models around empirical data of how incidents tend to evolve over time, and looking at that repository of thousands of incidents. We've built the models of the differences, but also similarities around different types of insider incidents. And really, what we're trying to do is to raise awareness of how those incidents tend to evolve over time, to assist organizations to identify some of those potential risk indicators, and really, looking at the behaviorally-based risk indicators, as well as the technical-based risk indicators. So if you are interested in those models, those are available on the Software Engineering Institute website. You can certainly do a search for insider threat or insider risk, and that provides a lot of the foundational work, the years of research, around building those models, looking for some of those patterns, looking at some of the potential risk indicators to individuals, to organizations, and really trying to build some of those preventative, but also detective, controls into those processes. So much more information is available on our website. And where we are today, Dan, 20 years later, you know, really, can you maybe summarize what has changed, or has it changed? Any of the current research or proposed research going forward, is there really anything that's significantly different from the foundational work which was done almost 20 years ago, to where we are today? What are your thoughts and ideas about what's new in insider risk identification, but also insider threat mitigation, for you and your team?

Dan Costa: Yeah, so a really good question, Randy. I think a couple of things to point out. In 2021, we are awash in data sources and technical controls that can help us kind of identify those individual potential risk indicators that our organizations associate with an increased risk to our organizations' critical assets, as posed by insiders. And where we are still at, both on the research and practitioner sides, is finding the right combinations of those potential risk indicators, to put together in ways that we can quantify risks that insiders pose, relative to the ways that we quantify risks, all other risks, within our enterprises. And the other thing that has changed is, with all of that data comes lots of different ways to make measurements.

And on both the research and engineering sides of our bodies of work, we're spending a lot of time helping organizations not only enumerate all the different combinations of data sources and analysis techniques they can apply to the potential risk indicators that they've identified, but which is the best, and then trying to find ways to quantify what we mean by best. There's cost considerations that need to be brought forward when we're trying to come up with what we mean by best. There are concerns about, is this the most accurate representation of that information, right? So we always like to use the example of (inaudible) records, the best place to go to try to gain an understanding of someone's time and attendance. You could probably gain a time and attendance metric by checking how frequently someone's logging in to chat, but if they didn't log into chat, but they were in the office, right? So it's different ways to make the same type of measurement, different data sources and analysis techniques we can apply.

So one of the things that team is hard at work at, in collaboration with a variety of different government and industry partners, is really bringing to bear that experimental evidence that shows, if this is the potential risk indicator you're looking for, you know, these are the different ways that we tried it. This is what works best in this organizational context. This is what works best in this other organizational context. Here's why they're different. Here's how you can figure out which one is most effective for you. So a lot of what we've done with regards to those foundational models that we've developed over decades, kind of analyzing incident data, the models still hold. Where our challenges are in 2021 is a) continuing to augment those with additional understanding regarding the relationships between those individual potential risk indicators, continuing to understand the best ways to quantify and measure a progression of an insider incident, from personal predispositions and stressors, all the way through kind of the harmful incident itself. And in trying to get better data into the hands of managers, resources, security practitioners, C suite, better data into the hands of the folks that will make risk-based decisions on what to do with the concerning behaviors and activity that we associate with increased risk with organizations' critical assets, as posed by their workforce. What to do with that information, how to get it into their hands faster, how to help them make better data-driven decisions faster.

Another thing that is-- another kind of good news-bad news deal, with regards again of what's new or where we're at in 2021 with insider risk management is, we're awash with vendor solutions, or bits and pieces of the problem, or even, you know, when we think about the emergence of dedicated, standalone insider risk management capabilities that we've seen over the past couple of years, we're awash with a variety of different tools that we can bring to bear on not only our technical challenges, but again, providing us that data that can feed some of the positive insurance controls that we talked about in our research. So if the landscape was complicated a handful of years ago, with the emergence of user and enemy behavioral analytics capabilities, and how they aligned with things like security and information, event management system tools. The water's gotten even muddier with kind of the emergence of these standalone insider risk management capabilities, as well as the emerging set of tools called extended detection response capabilities, so those next generation steps. So for insider threat program practitioners, there's a lot of work that needs to be done, not only to figure out what data you've got within your organization that aligns the things that pose an increased risk to your organization's critical assets, but now we've got a variety of different solution providers and vendors that we've got to come up with sound strategies to be able to evaluate the efficacy of those controls against what our security objectives are.

So we find folks kind of struggling, a) with those tests and evaluation capabilities, b) with establishing the right metrics that aligned what it is that their insider threat programs are actually trying to do, and that's really been the focus of our research over the past several years and will continue to be, for the foreseeable future as well.

Randy Trzeciak: Well, thanks, Dan. That's certainly helpful kind of setting the stage of where we are today, compared to where we were a couple of years ago, versus 20 years ago. Back then, it was just raising awareness that insider threats need to be incorporated into kind of the risk identification and organization recognizing internal threats, alongside of external threats, and then raising awareness of malicious versus accidental, and really kind of raising awareness to the point now where we're getting moving from beyond the nascent program to more looking for ways to measure how effective we can be in an insider risk program, and insider threat program. Getting to the point where we start using the M word, the maturity level of the program to measure the effectiveness of that as well.

So one of the things that we do here, obviously, is research, and our goal is to publish, to the great extent possible. We certainly want to make the audience aware of the hundreds of reports that are available broadly across all of CERT, but also across all of the Software Engineering Institute. And then specifically for this webcast, over 125 reports are publicly available on the work we've done around insider risk identification, insider threat mitigation, and those reports are publicly available on our website. One specific report that we do want to call your attention to, which is one of the more highly, or in some cases, the most highly downloaded document on the CERT website and the SEI website, is the common sense guide to the mitigation of insider threats. Now we've done multiple versions over the years, and really what that is, is our best practice guide to mitigating insider threats in an organization. And so they hopefully, in the very, very near future, you will be seeing an updated version of that, which will be coming out very, very soon.

So one of the best practices that's outlined in there will provide a lot of context around traditional security controls. Looking at ways by which organizations may be doing things to allow access, to prevent access, as traditional security controls, but also looking at some of the tried and true methods, such as separation of duties, or dual control. Putting those things in place to hopefully reduce the risk of an insider committing some type of harmful activity within the organization. And most organizations will put those into business processes. You know, really ways by which we can have one individual do one step of a process, a second individual's required to do a subsequent step, that will allow some type of dual control to be put in place. Now a question did come in, Dan, from our audience member, specifically looking at the two-person rule, or that dual control or the separation of duties, and would like us, specifically you, to comment on, well, how effective are those traditional security controls, including the two-person rule, to reduce the risk from insiders in organizations? So can you comment on that at all, maybe tie it back to the common sense guide if you would, please.

Dan Costa: Yeah, so Randy, I'm going to almost read this one verbatim, because the phrasing of the question from Michael-- and thanks for the question, Michael-- the phrasing of this question is almost-- is the most interesting part of the question itself. So it's, how much does the use of the two-person rule reduce the risk from an insider? It's the exact right question to be asking. When we're talking about managing insider risks, the goal of-- the kind of our shift of our focus from mitigating insider threats to managing insider risk, is to really put forward the strategies and the techniques that organizations can use to answer questions like the one that Michael has presented here. We've always had incorporating enterprise risk management and making sure that insider threats are considered as a part of an enterprise risk management program. We've always had that as a best practice in the common sense guide you mentioned, Randy. What we've learned over the past several years is, you know, that is vitally important to the success of a maturing insider threat program.

As we've seen insider threat programs kind of start in the federal civilian agency space, meeting the minimum requirements for insider threat programs in response to executive order 13587, that said, this is what it means to have an insider threat program that's now required to protect classified information. So as we started there, and we moved past that into other organizations understanding that they needed dedicated capabilities to protect their own critical assets, not necessarily just classified information, from insider threats, what they found early and often was, okay, once we get good at being reactive, and detecting the mass data exfiltration events that are associated with a large proportion of the folks that are leaving our organizations with company confidential information, once we get good at recovering from the IT system sabotage that was committed by a disgruntled insider because of some set of unmet expectations, once we're past all those kind of reactive capabilities and the ability to recover effectively from an insider attack, what can we be doing proactively to identify the concerning behaviors and activity that precede those harmful acts, and what positive controls can we put in place to address the root causes of the disgruntled system administrator? Or what can we put in place to help departing employees understand about the intellectual property agreements they signed when they joined the organization? Where are those administrative and management controls that we could proactively deploy to help reduce the impact and likelihood of insider attacks? And that's where we started to see the real need to double down on the integration of an insider threat program, into the overarching enterprise risk management capabilities that an organization has. And in many places, we've seen the insider risk management program was kind of leading the charge as one of the first really big use cases that an enterprise risk management program could have took on, with regards to enhancing their ability to quantify risk, their ability to manage risks at a more granular level, at the enterprise level. So it's really been kind of a two-way street, and it's one of the reasons why we are shifting and re-emphasizing kind of insider risk management, where applicable, in a lot of our research, in a lot of our publications.

So that is the world's longest preamble, before I actually answer Michael's question. Michael, spoiler alert, this is going to be a dissatisfying response, but we can use the principles of kind of enterprise risk management to help drive towards the things that you would have to gather within your organization to be able to attempt to qualify or quantify how much risk can be reduced via insiders by the implementation of something like the two-person rule. The way to break this down, or the way to slice and dice it is, okay, we're talking about enforcing a two-person integrity check on some critical business process, right? Whether it's making sure that two people need to be involved in the provisioning of administrator level privileges to some sensitive network or system. Whether it's having two people in the loop to authorize the purchase that exceeds some amount, let's call it a half million dollars for a really big organization. Whether it's having two people in the business process that's associated with, you know, issuing some credential, like a driver's license, or a passport or something like that. You've got this business process that exists, and we're talking about now trying to-- now because we're focused around this specific business process, we can dive in a little bit using tools like conducting business impact analyses, and say, okay, let's say that the normal way of creating a credential here isn't followed. What's going to be the impact of some back door account being created by some rogue system administrator, or someone who's been coerced by an external third party to create some back door access into their organization's network or systems, misusing their existing administrator level privileges.

So now that we're focused in on either a specific business process or a specific system, now we can start thinking about quantifying the impacts to a disruption of the confidentiality, integrity or availability of that specific business process. So once you've figured out what you're applying that two-person rule to, you're close enough to the assets that will sustain and support that business process, now we can start leveraging our tools from risk management to include a lot of the work we've done here within CERT and SEI, using methods like the OCTAVE method and the OCTAVE FORTE method, to help you identify and characterize the value of the assets associated with that business process and the potential impacts to the value of those assets that some degradation to the confidentiality, integrity or availability of those assets would incur.

So you're right, you were right. You're barking up the right tree, and the trick to being able to answer that question for your organization is really gaining an understanding of the business processes that are associated with the two-person rule that you're looking to deploy.

Randy Trzeciak: Thanks, Dan. And I certainly want to encourage the audience to continue submitting your questions. We'd love to take them live during our session today. And certainly if we can't get to all of the question today, we will attempt to follow up after our session does end today. So please keep the questions coming. We do want to make this an interactive dialog going forward. And really, one of the key points that we've tried to make since the early days of our insider threat research, and as Dan described, as you're trying to protect your organization's critical assets from all threats, external and internal, malicious and non-malicious. And as Dan perfectly described, that that's different in different organizations, and really based upon your ability to fulfil the mission of the organization would identify some of those critical services that need to be maintained, those critical business processes. And then specifically, looking at the assets around the four general categories that's adequately described in CERT's resilience management model, of protecting the facilities, the people that are in the facilities, the technologies that provide the cyber access, as well as the information, whether it be physical or cyber as well. Really focusing in from that point on what you're trying to protect. And in our foundational training that we provide, recognizing there's a different between insiders in your organizations, insiders that pose a threat to those critical assets, and the ability for you to prevent insiders from causing harm, which will be the insider incidents. Really focusing on the insider incidents as what you're trying to prevent, and then working your way back from there, reduces the potential likelihood that everybody is a threat to everything, and that's really not realistic in any organization.

So the foundational concept has been really in our training since the early days of the work we've done, recognizing there's a smaller set of individuals that actually do pose a threat and then focusing specifically on the prioritization of the assets should be the foundation of your insider risk or insider threat program. So yeah, it's a great question, and certainly tying that back to this formal method, such as OCTAVE or OCTAVE Allegro, is a great way to start. And if you don't have that asset inventory tied to prioritization, that's going to be the starting point of any enterprise risk, including insider risk identification as well.

So as we move on to a couple of other topics, we wanted to kind of bring to light, to add for discussion, certainly the world is in about month 18 of the pandemic, and certainly a lot of organizations have shifted to a more remote workforce where most of the workforce is not physically in that facility that we mentioned a couple of minutes ago. We have the remote workforce that's doing all of the critical systems, all of the critical business processes from an offsite location. And certainly, Dan, as part of you and your team's support for organizations, whether that be in the form of insider threat program evaluations or doing some type of other security assessments, have you seen any particular trends in insider risk, now that a lot of the workforce is remote? Anything that you've seen organizations do particularly well or areas where organizations may have been challenged over the past 18 months? And what would you anticipate would be the likelihood going forward of a continued remote workforce and its impact on insider threat mitigation?

Dan Costa: Yeah, good questions, Randy. I'm going to decompose that a little bit, and then you keep me honest about whether or not I've gotten everything that you wanted us to cover.

Randy Trzeciak: Mm-hmm.

Dan Costa: Going back to some of the fundamental models that we've developed with regards to insider incident progression there, say, the foundational pieces around stressors, personal stressors, professional stressors, financial stressors, all sorts of different things that happen to people in their lives, that through the incidents that we've studied, increase the likelihood of unauthorized use, or misuse, of an organization's-- of authorized access to an organization's critical assets. So safe to say, over the past year and a half, that the work force en masse has been exposed to a significantly higher number of stressors, be they personal or professional than we were used to seeing in years prior. So the hypothesis from our side, from the research side, was an uptick in stressors will lead to an uptick in the risk that insiders pose to an organization's critical assets. Through the work that we've done and the program evaluations and vulnerability assessments, as well as just the feedback we're getting from the community through our public training courses, through our open source insider threat community of practice, we have seen, it's going to be a noticeable uptick in the types of insider insights that organizations experience.

What we've also seen, and this is the first few months of the pandemic, was some pretty stark reminders of the limitations of a lot of the capabilities that our insider threat programs use to wade through and make sense of the mountains and mountains of data that insider threat programs can collect and are exposed to. And that had to do with anomaly detection. The mechanisms by which we can, you know, in some automated or semi-automated fashion, generate alerts that show us when a deviation from some normal or expected condition occurs, whether that is a change in an individual's kind of work hours, the ways in which they're interacting with our organization's network or systems, how much data they're downloading or uploading. Use anomaly detection capabilities here as kind of these front line detectors, to give us an understanding of, okay, something has changed here. Can we identify what the root cause of this change is, or is this associated--? This anomalous uptick in your data downloads, is this associated with a mass data exfiltration event? What we found, when everyone's normal, or everyone's baseline shifted in March and April of 2020, was those tried and true methods for detecting anomalies, and kind of their relationship between anomalous activity and actual insider threat behavior completely shifted and completely flipped upside down. And for the first several months of the pandemic, once we got everybody connected back to our VPNs and got that telemetry feeding back into our insider threat programs, we saw lots of organizations struggle with, how quickly can we re-baseline what normal is? So that we can then start detecting deviations from normal, from what is everyone's new normal.

So we learned a lot about how much to rely on anomaly detection capabilities and how to incorporate the idea that everything is going to look anomalous a while, for a while, into that insider threat analysis capability. And those lessons learned are going to be really important for organizations as the inverse happens, as we start to see folks, over the next month, months or year, or years, trickle back into the office. Now our anomaly detection capabilities are going to have to be able to withstand another massive shift, and what normal looks like for our organizations. And as you mentioned before, a hybrid workforce, if that's what ends up happening, will only layer on additional complexity with regards to how we characterize anomalies. So what we've found is folks working closely with their solution providers, with the folks that help them generate these alerts, with their insider threat analysts, on kind of right-sizing how we do anomaly detection, how much data we need to be able to collect before we consider that kind of a baseline of somebody's normal. We were traditionally relying on 30, 60, 90, seeing up to 180 days of kind of prior data needed to be able to build a baseline. What we figured out a year and a half ago was, that's too long to wait to be able to kind of re-establish what normal looks like for insider threat program operations. So it's that lesson learned, and those lessons learned with regards to kind of how best to utilize things like anomaly detection that we're seeing organizations start to consider and adopt and adapt to, as they plan for, and anticipate another shift in their workforce back from fully remote.

Randy Trzeciak: That's a great insight, as organizations will prepare, hopefully, for a re-entry into a physical workplace as well, or as you managed-- as you described, managing a hybrid. Seems like that'll be certainly the short term, maybe medium term, or even long term as well, but really, the goal from anomaly detection standpoint is to do exactly as you described, in recognizing that not all anomalies, as it is described, is malicious. You know, just something different from what's expected, in those baselines where you need to train your insider threat analyst to hopefully identify alongside of the tools what are the anomalies, do that triage process based upon some guidelines or thresholds to begin possibly an inquiry. That inquiry then has some process that needs to be followed that could potentially lead to an investigation, but at each of those stages, have your insider threat analyst work with your insider threat program managers, and the counsel that provides the oversight and governance of the program, to provide insight into what those anomaly detection capabilities will be, but also what those thresholds to move from an anomaly to an inquiry, inquiry to investigation, and possibly investigation into possibly prosecution at some point. And that would be as we move beyond just a tool detecting anomalies to the more maturity of the programs. And then certainly, as we've talked about through a number of these webinars and publications, you know, the unintended consequences of programs, how it will impact individuals, particularly if we don't have that very formal process to follow from anomaly to inquiry, inquiry to investigation, and we want to certainly protect the privacy and civil liberties as we're doing these insider risk identification efforts as well. So I do appreciate, Dan, kind of using those formal methods, but tying that into the formality around insider risk and insider threat programs as well.

Dan Costa: Yeah, there's something else coming on the horizon, Randy, that insider threat programs need to be acutely aware of, and it kind of ties into this anomaly detection conversation we're having. Lots of global workforce climate surveys that are being published over the last couple of months suggest that up to half of the workforce could be considering and taking a new position, or leaving an organization over the next year. And as our data tells us over the incidents that we've studied, departing employees pose increased risk to organizations' critical assets. They either, with malicious intent, or by accident, or due to a lack of awareness of intellectual property policies, or the company procedures of retaining information or retaining hardware. That increased movement in and out of the workforce is going to pose additional challenges insider threat programs are going to have to adapt to and consider, right? And it's not just on the, okay, someone's leaving. Let's put a bunch of technical detection capabilities in place to make sure they're not stealing from us on the way out. But it's also on the retention side of the house. And these are the things that we talked about. We're talking about a balanced approach and positive insurance, but how can the organization change its culture, its management practices, to retain those employees that have years of service there, and continue to make the workforce, the organization, an attractive place to stay, while all of this movement is happening, kind of into and out of other organizations?

So things we don't typically think about as security controls as we prepare for this kind of mass potential migration of the workforce, will become effective tools for not only the security practitioners within an organization, but the organization's effectiveness as a whole.

Randy Trzeciak: Okay, thank you. So then we do have one question that came through, through Chad. I'd like to propose it to you and then maybe you can discuss it for a minute or two, about the effectiveness of adverse information reporting when it comes to mitigating insider threats. Have you seen organizations that are effective at doing that? Looking at information, discerning the quality of the information that's coming? You mentioned earlier the data sources. There's a number of technical data sources, but also information that may be coming through confidential reporting, or maybe anonymous reporting. Some of that information may have not been verified to the point where it is truly helping to mitigate risk in an organization. So have you thought about that or done any research into the adverse information reporting and its relation to insider risk mitigation?

Dan Costa: Yeah, we've been fortunate enough to work this problem from a couple of different angles. One of the first places we started was really in kind of a thought experiment, and a little bit of research we did around the potential pitfalls of an ineffective insider threat program, and what insider threat programs to kind of run off the rails would potentially do, and what types of pitfalls to look out for and avoid if you're trying to build an effective insider risk management capability. So there's a great paper out there, led by one of our researchers, Andy Marr, called "Effective insider threat programs: understanding and avoiding potential pitfalls." And in that paper, one of the places that we spent some time talking about are ways to leverage the workforce as input into our understanding of the concerning behaviors that might be happening across the workforce, even the stressors, to give us a chance to positively intervene within the employees. What happens if you do that wrong is, you do things like encourage snitching behavior, or unduly portray this sense of big brother, or this overt spying on our employees, without a real basis for that kind of curiosity, or that kind of skepticism. It's a really quick way to alienate your workforce, make them less productive, and also erode any buy-in or support for the organization's insider threat program more broadly.

On the opposite side of the spectrum, we've been fortunate to work with organizations who are employing and deploying these employee appraisal tools that are administered to managers and supervisors, that are designed to help managers and supervisors gather information from their employees, and just from the day to day management of the workforce, to help them not only think about the increased risk that somebody poses to stealing from us, but where folks are overworked, where folks are feeling disconnected from the workplace, where folks are in need of some of the support services that our organizations provide via credit counseling, employee assistance programs. It can help managers gather the information from their employees that help them more effectively manage their teams and manage their people. So it really does run the gamut of our work in this, which is spending time thinking about and hearing from folks that have kind of done this the wrong way, and learning from them with regards to how to avoid that, all the way towards leveraging the workforce and management as input into the insider risk management program, that really gives us that opportunity to proactively deploy these controls that we normally think about when we're talking about positive returns.

Randy Trzeciak: Okay, thanks, Dan. So as we're looking towards the end of our session today and we have a few minutes left, I do want to circle back to, you called out earlier an acronym for EDR, extended or endpoint detection and response, and you kind of tied that around integration with host-based monitoring, or entity behavioral analytic type tools. Certainly, could you maybe describe your thoughts and ideas of how an EDR, as a tool, might contribute to the tool suite that organizations have when building insider risk mitigation programs and organizations?

Dan Costa: Yeah, so it's next generation security information and then management. And what that means is, you know, bringing to bear some of the capabilities that we're missing from the previous generation of gathering data from disparate sources, and then being able to query that data in its aggregate, in a more granular fashion or in a unified fashion, to allow us to, you know-- with a little bit more analytic flexibility, be able to identify those potential risk indicators for insider threat programs to consider.

So what's new? What's new is not necessarily new. It's bringing in bits and pieces of capabilities from other tools, like user and behavioral analytics capabilities, which extend how we do alert-based detection in a security information event management system by associating all of those individual log activities with a user, or with a user account, or with a machine, right? Some other entity associated with that. The other thing that you'll see kind of in the next generation security information event management systems is more by ways of letting you use advanced analytic capabilities, like our official intelligence and machine learning, as the foundation for your anomaly detection, as inputs into a broader risk scoring capability, and more by way of just security orchestration. How do we better integrate these capabilities with our risk registers, our data loss prevention tools? How do start to kind of stitch together all of these different capabilities that form the fabric of our detection, prevention and response infrastructure?

So just another set of tools to throw onto the pile that insider threat program managers and CISOs need to kind of come up to speed on and consider, and our recommendation for this is always, evaluate your needs on a use case by use case approach. Don't go flying to the shelves to grab that capability that is the new or the next generation without a careful and thoughtful evaluation of the capabilities that you already have in place, and what your capability gaps are. What can't you measure as effectively or efficiently right now than you wish you could? And once you've got those use cases and requirements articulated, then you can start to find ways to most cost effectively and efficiently address your capability gaps. There's so much overlap between these tool categories in 2021 that you can't just run to the shelf and grab an IRN solution and be done with your insider risk management program. There's so many interdependencies and data prerequisites that are needed, and so much variance between what is in scope for your insider threat program, and what already exists within your organization by way of data sources and controls, that it really does require that use case-based approach when you're trying to fill your technology needs.

Randy Trzeciak: Yes, certainly, Dan. We've talked over the course of a number of years about the insider threat tool or tool suite is not the program. It's a component of the program and really when a new organization is too fast at acquiring a tool before they know what the tool is to be used for, or what incidents you're trying to prevent, that it's certainly putting the cart before the horse. Recognizing as part of our training program, going back to that organization mission, the critical services, the critical assets. Trying to prevent someone from stealing intellectual property would require a set of tools that would be different from someone trying to prevent, or someone from trying to commit fraud against the organization, which would be different from someone trying to sabotage the IT systems, which would be different from trying to prevent someone from doing unauthorized disclosure, or in a government realm, espionage-type activities. So really, tying it back to that enterprise focus of what are you trying to prevent? Which type of harm are you trying to prevent? Which type of assets are needed to be contained in terms of confidentiality, integrity and availability? Then knowing that, the prioritization of the assets, then you can start selecting tools that can help to try to prevent that harm from being realized by an organization. So as we've said, information technology has a seat at the information risk management enterprise risk focus, but also equally does physical security, as well as the other parts of the organization, human resources, general counsel, as well as the risk focus components of the organization as well. So it's a holistic program across the organization. Information technology helps to support the program, but it should not be the sole focus only of a program as well.

So Dan, we did have one question that did come in as we were talking in the previous section, looking specifically about the departing employees. You talked about-- you know, mentioned about workforce that are moving on. Do we have any potential causes or reasons, or reason to believe why are people leaving organizations as a motivating factor that could help to inform insider risk mitigation in organizations that may experience a significant or even a slight movement of workforce out of their organization?

Dan Costa: It's a good question. Depending on which of those kind of global workforce climate surveys you're looking at, you're looking at-- and you'll see a couple of things kind of bubble to the top. Some of them have to do with changes in the organization's policies regarding remote work, right? Some of them have to do with just personal and professional development goals that aren't being satisfied within the current organization. The pandemic kind of enlarges-- you know, had a lot of people spending time thinking about what the future looks like for them, once we get on the other side of this. You know, a lot of that comes with, are there other opportunities for me outside the workforce? So the point is, depending on which of these surveys you're looking at, you'll find a bunch of potential suggestions for kind of the primary motivators or primary root causes. What's important for insider threat programs to understand is, getting to those motivators or what might be causing mass employee movement activities within their own organizations. Here's my hypothesis. Those motivators might vary significantly from one organization to the next, depending on their policies, their procedures, their culture. So it's important for an organization that might be experiencing an increased uptick in their workforce kind of departing, is rolling up their sleeves and getting an understanding of what some of those primary causes are, and getting an understanding of what the security implications of those are. This goes again back to some of those positive deterrents, balanced approaches that we were talking about. What you'll find is, potentially the insider threat programs having the opportunity to influence decisions on hiring and retention practices that are happening within the organizations, because of the unique collection of data that the insider threat program team has access to.

So this very much is an example of how insider threat program operations can be used as a two-way street. They're not necessarily just providing information to HR to help them with a very specific part of their day to day needs, onboarding, offboarding. But being able to, by working in partnership with them, helping them leverage the data the insider threat program collects via authorized means, to gain better understanding or insights into kind of how the workforce is feeling, acting and behaving as a whole, and then certainly understanding the security implications of that.

Randy Trzeciak: And certainly, as we've tried to identify higher risk times for organizations, we've seen that departing employees, as you described earlier, the risk that an employee could take something with them when they leave, as a way to provide some business advantage, we've cited in a previous report specifically looking at theft of intellectual property, based upon the data we’ve collected, the incidents we've analyzed, that as high as 80 percent of the people that took intellectual property, stole the intellectual property, did it within 30 days of announcing they're leaving the organization. So a higher risk time, in terms of departing employees, and the recommendation is that if we can identify people early enough to do some possibly additional monitoring, do you have the ability to monitor for the time they, for example, announce they're leaving, to the time they leave, to look to see what they may be downloading or sending off of the corporate network? But also looking back before they announce the resignation, that's where we get that 30 day window of potential opportunity for detection of someone stealing intellectual property. So what we try to do is to provide that actionable guidance around the actual timeframes of when it's more likely that someone would be motivated to take, for example, intellectual property from an organization. So you can certainly refer to that report, as well as a number of other reports specific to theft of intellectual property, information technology sabotage, defrauding an organization, unauthorized disclosure. Those would be the malicious insider incidents. And we also have reports on our websites for the accidental or the unintentional insider threats as well.

So as we come to the conclusion for our session today, we certainly want to raise awareness, again, of the research that we've done, the work that is publicly available on our websites. We certainly point you to the Software Engineering Institute's websites, specifically the CERT division, and more specifically, insider risk that we've done. There's a significant amount of reports and information available as well. So Dan, in our final few minutes, I did want to turn it over to you to really just, any other thoughts or ideas? Anything else that we could have or should have covered? Any closing remarks before we call a wrap to our session today?

Dan Costa: Yeah, just maybe a couple of quick plugs, Randy. Anyone interested in registering for the symposium can find a link from our website, sei.cmu.edu. Randy, you mentioned the common sense guide as one of the hallmark publications of the team. We're putting the finishing touches on the seventh edition of that, this time called "The common sense guide to managing insider risk", which will include the twenty-second best practice that our research has identified. So stay on the lookout for that. We hope to be able to share a link with that, with all of you on September 28th and 29th. And thanks for the questions, and looking forward to continuing the discussion later this month.

Randy Trzeciak: Again, I did want to maybe just ask one more, a point of highlight. You mentioned earlier the OSIT group, the open source insider threat working group. If you wouldn't mind, maybe just give a brief overview of what that is, and how someone might get additional information on that. That would be helpful.

Dan Costa: Sure, yeah. So we maintain here at the SEI, we maintain a community of practice, of insider threat program practitioners from industry. It allows us as a DoD (inaudible) to gain an understanding of kind of what the best practices are in industry that might be applicable to DoD insider threat program operations, as well as applicable across the federal civilian agency space. So the group has been around for almost a decade at this point. Six hundred program practitioners strong. We meet monthly on the phones and usually once a year, either in person or virtual, to talk shop, just share lessons learned and best practices within that community of practice. And the industry practitioners interested in joining can find more information on our website, or send an email to osit-forum-support@cert.org.

Randy Trzeciak: Okay, thanks, Dan. So as we come to the conclusion for our session today, I certainly want to thank Dan for his contributions for our session today. But also to recognize the great work that he and his team are doing in insider risk mitigation. Certainly the foundational work is based upon research. The empirical data is the foundation for all that we do, but also working with operational programs to help to measure, to implement strategies for measurement of the effectiveness of programs, and we certainly want to recognize the work that's being done by Dan and the team. The team, including the researchers that were called out earlier today, of the great work that's being done. So thanks to the team. Certainly, the support of the Software Engineering Institute to continue this research for going on 20 years, and actually over 20 years, that's been foundational, as we look to truly help organizations protect their critical assets from all threats, including insider threats as well.

So it's been a privilege for me to kind of moderate this session today, being part of the insider risk team over the course of a number of years, and it's great to certainly call out and make available to you resources that are publicly available. So just as one final reminder, going to the Software Engineering Institute, sei.cmu.edu. You can find this work as well as other work that's foundational to protect in the national interest here in the United States, but also internationally from all threats to critical assets. So it's been a privilege to be with you today. Thanks again, Dan. Shane, I do want to turn it back over to you for any final closing remarks. So back to you, Shane.

Shane McGraw: Dan and Randy, thank you for a great discussion today and sharing your expertise. We greatly appreciate it. Also we want to thank each and every one of you for spending the last hour with us. Upon exiting, we ask that you hit that like button below, and share the archive if you found value today. Also, you can subscribe to the SEI YouTube channel by clicking on the SEI seal in the lower right corner of the video window. Lastly, join us for our next livestream, which will be September 22nd. Our topic will be AI engineering. Ask us anything about building better AI with Matt Gaston and Rachel Dzombak. Registration information is on our website now, and we'll be emailing it out as well. Any questions from today's event, you can send anything to info@sei.cmu.edu. Thanks everyone. Have a great day.