SEI Webcast

Amplifying Your Privacy Program: Strategies for Success

by Dan Costa and Carrie Gardner

Shane McGraw: Hello, and welcome to today's SEI Webcast, Amplifying Your Privacy Program: Strategies for Success. 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 today as interactive as possible, so we will address questions throughout today's talk, and you can submit those questions in the YouTube chat area, and we will get to as many as we can. Our featured speakers today are Dan Costa and Carrier Gardner. Dan is a technical manager in the CERT Division here at the SEI. He leads research and engineering efforts of the CERT National Insider Threat Center where he and his team conduct empirical research, develop solutions that enable organizations to effectively manage insider risks. Carrie's a team lead of the Insider Risk Great at CMU's SEI where she researches, develops, and transitions evidence-based solutions to mitigate cyber risks. She's principally focused on insider threat risks management, and applies a cross domain lens of psychology, policy, and information science to assess and address the multidimensional risks posed by insiders. Now I'll turn it over to Dan Costa. Dan, good morning. All yours.

Dan Costa: Shane, good morning, and thank you for the introduction. Hello, everyone. Thanks for joining us out there. Excited to be with you today to discuss all things, privacy program planning, implementation, as well as share some lessons learned and best practices that we've discovered in this space as we conduct our research and development efforts here at the SEI. I'm very happy to be joined this morning by Carrie Gardner, one of our subject matter experts in this space. Carrie, good morning, welcome.

Carrie Gardner: Good morning, Dan. Thank you for having me. This is a really exciting space. I'm very happy to be able to talk with you this morning about what is the current research that we're doing in privacy program, operations, and where we're looking towards the future in creating these evidence-based recommendations and opportunities to leverage the state of the art in privacy program practices and operations. So this is a really exciting area.

Dan Costa: Certainly. And I want to echo some comments Shane made in the beginning remarks for this webcast. We are really hoping to turn this into an interactive conversation with you all out there. Carrie and I have some materials prepared, and are looking forward to having a discussion about kind of where things are right now with regards to privacy programs, where there might be challenges and opportunities for growth, and where we see kind of the research landscape around privacy program planning and implementation, but certainly encourage your thoughts, your ideas, your questions. We want to keep this as interactive as we possibly can. Carrie, why don't we get started today with a discussion of kind of where things are right now

with regards to the state of the practice for privacy programs. Why don't you kick us off with a couple of thoughts with regards to kind of where things are and where some of the challenge problems or growth opportunities might be?

Carrie Gardner: Absolutely. Yeah. So actually, I just received the International Association of Privacy Professionals Certified Information Privacy Manager's credential.

Dan Costa: Congratulations.

Carrie Gardner: Thank you. So this has been on my mind recently, and it's also on my mind because as the new team lead for insider risk, we do come across interacting with privacy professionals a lot across the different types of organizations that we work for, so everyone from the public sector working for a federal agency to working in industry and helping them and enabling their insider threat programs. We're constantly getting questions on what's the best way to integrate insider threat risk management in privacy efforts. So this is a topic near and dear to my heart. And something that I've been noticing more recently is very compliance-driven. So Dan we within the Risk and Resilience Directorate here at CERT, and so we're constantly kind of coming from this from thinking about how can we manage our risks to kind of transition to a resilient posture. And right now, from the privacy perspective, a lot of this is focused on kind of closing this checklist of requirements. So what are some set of controls that we need to have coverage on? What are the reporting requirements if a data breach were to occur? And with that perspective, being on the compliance side, it gets very tricky in terms of prioritizing your efforts and your operations, particularly when we consider the regulatory patchwork by which privacy is in the middle of. So not just in the U.S., but even internationally. It's a very integrated landscape. So on the U.S. side, we have sector-based regulations, everything on healthcare, finance, types of data that need to be protected. On the U.S., like the national requirements, it's something where we don't have a national regulatory framework like GDP or like Brazil or Japan's regulations. So when organizations are moving forward and operationalizing a privacy program, navigating this jurisdictional landscape does become a challenge. So one of the conversations we've been having is how can we transition this to a risk perspective, leading into risk management on privacy.

Dan Costa: Yeah. So, you know, Carrie, I think just wrapping your head around the things that you have to do as an organization to be in compliance with all of the different requirements you might have from a privacy protections perspective-- I mean, I don't want to downplay how hard of a challenge just that is. One of the barriers for organizations taking kind of a more proactive approach to kind of considering privacy risks is just how hard it is right now to kind of keep up to

date with all of the things that you have to do to make sure you're not breaking laws, to make sure that you are not satisfying, or that you are satisfying kind of regulatory requirements, and that you're staying up to date with regards to kind of what policies and procedures internal to your organizations need to be developed to ensure proper privacy protections are in place across all of the different lines of business and all of the different parts of the world that large and complex organizations might be operating in. So the scale and complexity of this challenge continues to kind of increase at a rapid rate.

Carrie Gardner: Yeah. And so just even looking at the U.S. alone, states are moving forward with their own regulation pieces that actually are building upon existing state data breach notification laws. So nearly every state has some definition of what is a data breach. And so that actually has a legal hook in terms of requiring reporting to the individuals, to entities, and it varies by state-by-state. But laws like the California Consumer Privacy Act, the CCPA, build upon that, add a broader definition of PII, and then also speaking [ph?] to organizations that are not centrally located in California, but happen to have consumers in California. So that becomes an additional challenge for a national brand that is based in Texas, based in a different state, but has consumers in California. So these types of regulations are coming out it seems with more frequency, and so with that, organizations are now having to pivot and be more agile in terms of managing the compliance side of the risk and also looking forward in terms of thinking about how can more efficiently operationalize these practices.

Dan Costa: Carrie, you mentioned data breaches a few moments ago, and I think they're a really good example of the third bullet have listed here on this slide, which is kind of a gap between kind of policy developers and the practitioners that are responsible for doing things like understanding when a data breach may have occurred within our organization. So one of the things that we've seen kind of operationally is differences in understanding, differences in availability of information and data between kind of privacy program practitioners and the folks that have hands on keyboard, eyes on glass that are doing things like trying to monitor for the presence of evidence that suggests data breaches within our organization. So it can be challenging even within the same organization to get everybody head nodding in agreement with regards to what constitutes a data breach and is a particular collection of information something that meets that definition that we're kind of working with internally.

Carrie Gardner: Absolutely. And I think that's where we can really use our technical expertise to help drive this conversation and help educate different types of audiences, because there's a gap between the policies and here are the privacy values that we've passed and codified in a regulation piece. And in terms of implementation that in an organization, then you have to think

about codifying the set of policies and practices and procedures. And then we actually have to operationalize that in a practice, which there's a training component and then there's a common language component. And so we can use our technical expertise here, particularly on the security side, to inform the conversation of here are the different types of controls, here's is what's happening on the data collection, data processing side, and here's potentially a gap. So I think we have a lot of opportunity, particularly within Insider Risk to help identify for privacy stakeholders. Here is an example of PII that is being adjusted into a tool. Here are different types of processes for instance with some type of risk calculation for insider risk, or another form of data science or machine learning, and here is the potential risks associated with that. And so that actually brings me to a good point, that NIST last year released a privacy risk framework. So it's kind of like that analogued the cybersecurity framework, but focused on privacy risk. And I took a walk through it recently, and was looking to see what controls are not accounted for. So with the NIST 800-53 Control Catalog, there's actually a nice crosswalk between the privacy risk framework and the existing control catalog. And there's three separate functional areas that are not accounted for in the NIST Control Catalog, and one of them related to data processing. And that's actually really critical for the work that we do, Dan, with insider risk in thinking about how data gets ingested in tools like a user entity behavior analytics application, and what happens to that piece of data. What are the transformations, what are the analytics that get put on top of it, and what types of risks does that pose for the individual? So I've had conversations with privacy professionals and organizations we're supporting, and they're still kind of wrapping their head around what's the difference between collection versus processing. And so I think this is a great area to inform that conversation.

Dan Costa: Absolutely. Again, just more evidence of the fact that kind of that gap between kind of the lowest level practitioners from a security perspective and the folks that are responsible for ensuring effective privacy protections kind of remain in place even within our security operations. A little bit of good news/bad news on that front, Carrie. This is not kind of the only place within an organization where we see kind of that disconnect, right? This is a common challenge that we face when we're talking about kind of taking the outputs from something like a security and information event management system or a host-based user activity monitor and capability and turning that into some measure of risk that can be actioned on kind of at the highest levels of the organization. There are sort of layers to translation and interpretation of the outputs of some of these tools that need to be performed until we can get that information in a format that is digestible for kind of our senior decision makers and our senior business leaders. So there's lessons learned that we can take way from kind of other challenges just in translation that we have within kind of our security functions and risk

management functions more broadly that we can certainly apply to privacy programming planning.

Carrie Gardner: Absolutely. One comment you mentioned on-- well, I was teeing off of is the human element. So what's the usability of these systems? One of our senior privacy engineers here who also has human interaction expertise, we've had conversations thinking about we have this piece of information, we have this screen essentially on the analytics solution. What's the best way to provide more notice, more controls, more support for the people and the users actually interacting with these solutions? So I also think there's room here on the research side to think about the operationalization of these solutions and how is the human in the loop staying informed of the potential privacy risks throughout the lifecycle of using the application.

Dan Costa: Yeah. I think that's a great example of kind of different approach to kind of privacy programs and privacy protections that organizations need to consider. And I think the point of a lot of the conversation today is really advocating for kind of moving away from kind of privacy as kind of this compliance-driven function, but ensuring that organizations are enumerating, quantifying wherever possible and being proactive about kind of thinking about privacy risks in an overarching enterprise risk management function. And that's something that we're starting to kind of see evidence out into operations with organizations who are kind of taking that plunge, adopting a little bit more of kind of a privacy risk focus to their privacy program planning and implementation efforts are starting to see good returns on initial investments upfront to do some of that leg work, as Carrie had mentioned, being proactive about kind of the identification of privacy implications and considerations across multiple lines of business within the organizations, not just the security function.

Carrie Gardner: Absolutely. So on this particular slide here, for instance, I have a graphic I pulled from a recent Cisco report. It was fantastic. It was on thinking about the risk side and the business justification of really investing in privacy programs. And they pulled out a few different opportunities that organizations can look to when they decide to really lean into the risk side of privacy management. And a few of these, they go to the cost effects of being able to really leverage and sell the work we've leaned into privacy. And some of these include reducing sales delays, mitigating losses, but also on the consumer trust side, building brand loyalty. So I think there's not just the compliance requirements and the motivators from thinking about we want to make sure we have all of our bases covered, but there's also consumer and business oriented motivators. Part of that-- on the for-profit side, that literally is building brand loyalty and consumer trust. But I also think on the public sector side that looks in the form of credibility, or it could be operational efficiency, right? So I think as we're looking to build more trust with our

employees, with the stakeholders that we have out there, they look to see how do you guys recover-- like how does the organization recover, right? So we all kind of in the cybersecurity world have accepted the fact that data breaches happen. But how do you recover? What's your resilience plan look like, you know? So making sure that they stay in active control of responding to a data breach incident I think really reflects well upon an organization.

Dan Costa: Yeah. Just to build on something you mentioned there before, Carrie, consumers are getting smarter with regards to kind of their expectations for how us as organizations are protecting the data that they give to us when we enter into business relationships with them. So we're seeing kind of pressure on the consumer side, or expectations shifting on the consumer side that are putting pressure on organizations to be more proactive with their ability to produce answers to some of the questions that they're getting. And as Carrie had mentioned, kind of this concept of trust, right, becoming increasingly more valuable for organizations, both public sector and private sector, to be able to better quantify, to be able to better manage and maintain kind of strong measurements on kind of as the risk landscape for the organization might change. So it's an interesting dynamic that you're seeing played out here. Some of the data that's coming in from practitioners kind of backs this up.

Carrie Gardner: Absolutely. And I also think this is a really good point to think about from an insider risk perspective is how can we really kind of change the narrative on the negative side of insider risk management and look to the positive side and thinking about building and engaging the workforce, right? We're building trust and hopefully in order to deter potential authorized users from carrying out an insider threat. And when the organization is able to point at things in the form of like privacy protections and ensuring that that data is safeguarded and that employees have control over their data, that's a good thing in terms of, again, building that reputation of how the organization is better protecting and safeguarding that sensitive information. And also it informs insider threat programs in working and coordinating better with privacy requirements and the privacy perspective of an organization.

Dan Costa: Yeah. I think the relationship between kind of insider threat programs, insider risk management programs and privacy programs, for organizations that have been successful at integrating those two capabilities are exemplar for how other security functions can and should be kind of interacting and being informed by kind of a privacy risk focus, privacy program within organizations. As organizations' security functions start to collect and analyze data in larger volumes through the utilization of kind of more modernized technology, insider threat programs for years have had to have kind of legal and privacy stakeholders as the invaluable early participants into the planning of insider threat program operations and activities to make sure

that the data that is being collected is allowed to be collected before we go ahead and start deploying new sensors onto networks and systems, but then also to ensure that the data that's being collected is being used in ways that are authorized and legal and in alignment with all the company policies and procedures. So there's lots that we can kind of take away from how those healthy relationships between insider risk programs and privacy programs are working that can better inform kind of things that are happening in other security functions within organizations.

Carrie Gardner: Absolutely. You made a point on thinking about the specification requirements for utilizing a data collection analysis tool, such as a user activity monitoring solution for or user entity behavior analytics solution. So by having a very strong privacy program that's coordinated well with insider threat that provides a way to share information on generating that use case-based specification for including tools like a UAM or UEBA. When privacy programs understand like these are the different threat scenarios, these are the different use cases for why we need a tool like this, and here's the limited scope by which that tool would operate, there's better understanding of the controls that would need to be put in place for that tool to be deployed and also to understand why this tool is justified. So I think there's a common misunderstanding between those interests, between insider threat and privacy, but a lot of that could be resolved by better communications and understanding that there are legitimate insider threats. There's a need to have a set of controls, but we also need to ensure that we're taking a risk-based approach in terms of implementing different monitoring activities or other forms of controls to be able to detect those events. So the privacy requirements of documenting that and justifying the data collection and processing specification requirements can be informed by having better privacy program and insider threat coordination.

Dan Costa: Yeah. It's a great point, Carrie. We've been spending a lot of time focusing on kind of security operations. But security options and security functions aren't the only parts of an organization that might be collecting and analyzing data about people, whether those are people that work for the organization or potential customers or consumers. I think a lot of what we're advocating for also works really well for privacy programs that are trying to wrap their head around what's happening in the marketing department with the kind of use of some new social listening platform, or anywhere else that we're kind of collecting information about individuals. We've been through this before in organizations that have kind of mature, robust and well integrated insider threat programs. And as different kind of parts of the business units that organizations might have start to adopt some different data collection and analysis techniques to support their business processes, it's a blueprint that you can already have within your organizations with regards to the questions that need to be asked and answered by the

folks that are collecting and analyzing that data from a privacy program protection and perspective.

Carrie Gardner: Absolutely, right? So there are some common processes that happen at the enterprise risk management level in terms of like doing a data inventory. And that's something that we ask insider threat programs to do, that we ask ERM programs to do. But privacy programs also have that. And so we have found that some of these efforts are kind of siloed into their particular teams and business units. And that's a good opportunity to reduce the duplicity of work essentially, and also to bring out these are the different data objects that we have across an organization. Here are the different controls that are in place, and here are some opportunities to better coordinate between groups and teams.

Dan Costa: Yeah. And, again, you're just highlighting like the hallmarks of a robust kind of enterprise risk management strategy. And the important takeaway there is privacy folks need to be involved in those conversations so that privacy risks can be adequately captured with regards to the business processes the organization is using to satisfy its mission. The data that's being collected and analyzed by different types of individuals within the organization, right, will pose different types of privacy risk. It's important to have the right stakeholders engaged on both sides when we're having conversations about kind of the actual risks to our organizations based on a myriad of different processes, both business related and security related.

Carrie Gardner: Absolutely. And so that actually makes me think of-- one of the FISMA requirements that may not get as much attention, but it's actually about privacy and it's about having agencies being required to have a continuous monitoring effort for privacy breaches and for privacy risks. So that actually gets wrapped up into the FISMA reporting requirements that get sent over to Congress annually. And part of those accounts for being able to have a risk catalog, or a risk register, if you would, of all the different areas of privacy, everything from the data collection, the processing, the documentation on the government side and ensuring that there is, in some ways, a checklist, but to have that enumerated out list of risks and where is the organization relative to that itemized list. And so that's a way to think about the fact that there are ways to collect this information routinely in a continuously format and thinking about this as a lifecycle, right? So kind of keeping on this privacy monitoring to monitor this risk throughout, like as a continuous process and not just an annual assessment necessarily.

Dan Costa: Carrie, really good points. Maybe a follow-on question there. Can you walk us through kind of who is responsible within an organization for kind of making sure that this is kind

of an ongoing process? Not to lead the witness, but it's likely not just the privacy program, right?

Carrie Gardner: Yeah. Yeah. And so that's why-- and this particular graph on, the top half here, the ERM. So the privacy program officer generally is the official designated to take the lead on all things related to privacy. So in a federal agency, generally they have a requirement for a designated senior official. In some ways it's like a designated insider threat senior official, but their purview is privacy and making sure that the organizations are like meeting all of the requirements for compliance requirements. But that individual doesn't work in a silo. So they have a privacy program office. They have-- part of that program office maintains the continuous operations center, which works in conjunction with information security, with insider risk. And so that's a distributed-type relationship generally, but it's all housed within the Enterprise Risk Management Unit. So regardless of the org chart in terms of who does the privacy senior official report to, generally the efforts are all unified underneath information technology and compliance subunits within an ERM program.

Dan Costa: It's a good point, which is your mileage may vary with regards to what your org chart looks like, but this is kind of the recommendation based on kind of conversations and best practices observed from kind of privacy programs out in the field with regards to kind of who is responsible for playing what roles within kind of achieving some of these objectives within organizations. Carrie, you've got kind of the insider risk and privacy pieces kind of explicitly called out here for more than one function. Can you talk a little bit to kind of what the intent behind kind of showing it like this is?

Carrie Gardner: Yeah. Yeah. Because these risks, privacy and insider risk, they're cross functional in nature. So there's legal compliance requirements that they have to meet, but there's more general information technology risks across both insider and privacy. And so that comes in the form of being operationally efficient if an incident were to occur or if met the data breach definition, so thinking about prevention, detection, response; thinking about impacts to infrastructure, more broadly on the data itself and impacts to the data. So that may not come necessarily just in legal requirements to report or to follow through and provide some type of credit card monitoring service, but there's just like organizational asks asset risks. And so that's kind of why like I drew those out under IT, to kind of call attention to the fact that even if these compliance requirements did not exist, this is something the organization should care about. This is informing best practices and informing good strategies and operations to prevent and better respond to potential incidents. So as we've already talked about, it's not "if," but "when,"

and making sure that you're best prepared to respond and efficiently recover, generally, most [ph?] organizations want to position themselves for.

Dan Costa: Great stuff. Carrie, a question. What role does governance play with regards to kind of a privacy program or ensuring proper privacy protections, or that privacy risks are adequately managed within an organization? So we're starting to see this become a boardroom issue for organizations from a governance and oversight perspective. What guidance or recommendations do you have for folks that are trying to ensure that the governance mechanisms they already have in place are aware of these issues, aware of these risks and doing what they should be doing with regards to ensuring the organization is meeting the needs from a privacy protections perspective?

Carrie Gardner: Absolutely. Yeah. So it does need to start at the top. Generally speaking, the General Counsel's Office has a set of requirements. They're using the legal expertise and lens to be able to identify what are the reporting requirements, what are the control requirements, how frequently do we need to be audited, and a variety of other operational requirements. And so that informs the process in terms of like here is what we have to do, but that also should be fed into if there is a chief risk officer position, that person is able to take that information and then kind of navigate and prioritize the efforts that get delegated out throughout the organization. So what I mean by that is governance, thinking about policies, thinking about things such as a privacy notice on any technology or any user interface, like a website that a user may visit. So users are at least aware of what data is collected and processed. And then also thinking about internally a privacy policy. So what are the requirements and what are the practices an organization is going to use when collecting any PII or processing any PII? What are the requirements and procedures for conducting a privacy threshold analysis, or if that threshold is met, to follow-on with a potential risky impact analysis assessment or PM. And so on the governance side, you have to think about how is your executive C suite made up and who-- if there is a chief risk officer, what does that look like organizationally, kind of back to this org chart. And so I think part of this conversation would go back to making sure we have an understanding of what those requirements are, but also thinking about strategically what were those business justifications for moving this to a risk perspective, and then having someone like a chief risk officer who is able to kind of in information from the legal requirements as well as like the operational risk requirements or recommendations to make the most sense of a path forward. And what would that look like on the policy side? What would that look like on the governance and supervision of those efforts?

Dan Costa: Yeah. Another thing that comes to mind for me is what do we need to put in the hands of the folks that are responsible for providing that governance that ensures that they're asking the right questions at the board meetings, that they are doing their due diligence with respect to ensuring that a new line of business or some decision that's made with regards to the strategic direction of our organizations has been done with an eye towards managing privacy risks or even enumerating those privacy risks in the first place? So I think there's room for kind of increases in the training and awareness that's provided to cybersecurity governance and oversight training for things like board directors with regards to things to keep in mind from a privacy perspective as you're doing your duties with regards to ensure the organization stays legal, stays compliant with everything it needs to be compliant to, and that it is doing an effective job managing privacy risk.

Carrie Gardner: Absolutely. So another thing I have here on the bottom half of this slide is people, process and technology. Maybe this sounds a little business schooly, but I kind of think through this lens and trying to identify operationally what this looks like. So we've talked to the people side and thinking about this theme, a cross functional problem that there's lawyers, there's policymakers and policy-driven privacy professionals. There's technologists as well. They're not always necessarily using the same language to describe things. So NIST, for instance, in that privacy risk framework is trying to develop a standard language by which to describe things and to translate things, and I think like that's a good step forward in ensuring that everyone's on the same page. I also think this is a good opportunity to talk about process and technology, because these cross functional folks, they're doing different things and carrying out requirements for auditing, carrying out compliance requirements and security operations requirements. And in some ways there's overlap and there's some ways to leverage the fact that we're already fulfilling control requirements for the cybersecurity framework. We have to be in compliance for that. And so if we're getting coverage with this particular profile, all these different areas. This also puts us in a position to be at this space level for the privacy risk framework. And so this is a good point, thinking about control mapping and making the most use of the existing processes across groups.

Dan Costa: Yeah. That's a best practice we've learned on the insider risk side of the house over and over and over again, right? Don't start from scratch, because you don't have to. Don't reinvent the wheel, because you shouldn't. It's a very good lesson to be kind of applied in this particular example as well.

Carrie Gardner: Mm-hmm. And then finally I have technology here. So, Dan, we've talked a bit about this, but one of my interests in thinking about privacy is helping organizations navigate

a build versus buy _____ 00:41:05. So if they're looking to acquire a new technology-- maybe this is some type of Smart city technology, or it's an insider threat user activity monitoring solution. Whether they go about building a custom software application, or they're looking to acquire one through an acquisitions process, how can we support organizations in ensuring they're able to configure and apply appropriate privacy controls to that new technology? So what are your thoughts and thinking about supporting a build or buy decision and helping inform organizations that are looking to acquire a new product?

Dan Costa: Yeah. So regardless of whether we are going to buy something or build something, right, whether that is a new security control or a new capability to collect and analyze data to support some business process, right, it's important to not put the cart before the horse and just wave your hand over the type of tool or the category of solution that you're out to acquire and say, "Well, we need one of those, because it does the thing that we think we need it to do." Better articulation of your requirements and your objectives up front is key to being able to incorporate requirements for things like privacy considerations in. If you don't, then you are taught-- let's use the security example to drive this home a little bit. If you're having this conversation at the level of specificity of "We need a user entity behavioral analytics tool because we don't have one," well, it's going to be really hard to walk through kind of privacy risks associated with how that particular tool that you're about to go acquire can collect and process data, how much data and when, it's shown to analysts. It gives you the inability to walk through kind of with regards to the analysis process. Are we constraining ourselves to a specific analysis process that might actually increase privacy risks or influence a bias piece of decision making, because we showed too much data to the analysts at a particular point. So if you're not down at that more granular kind of use case-based level for requirements specification and requirement solicitation up front regardless of whether or not you're talking about buying something off the shelf or going about building your own, you're going to be fail to have the opportunity to address some of these risks up front proactively. That's the most important thing that we've certainly seen within kind of insider risk control selection, insider risk control development is the need to best-- or as specifically as you can, articulate your requirements and how you intend to use these technologies. So you can start to think about where these technologies might be enhanced by privacy controls, where the requirements for privacy controls will fit in or align with how we intend to use this piece of technology to help us either support some business process or some security function. So that is kind of the most important part to that decision making process.

Carrie Gardner: Absolutely. Yeah. Being able to identify what those requirements are ahead of time if possible, that's the most critical time to build in or to require a set of requirements in the acquisitions process, for instance.

Dan Costa: And Carrie, if I could, it's also important for the lines of business, with the security folks, right, to not feel the burden to go about finding all of those requirements on their own or by themselves, or making them up, or assuming they've got full and complete knowledge, right? So that's where our privacy program stakeholders need to be engaged, right, in an active part of kind of the process with regards to requirements solicitation. So it's important. We've seen this happen within insider risk programs over the years, right? We've considered it, but we didn't necessarily get ground truth, or consult the subject matter experts within our organization, right? And because of all of the things we mentioned kind of earlier on in this conversation, how complex the regulatory landscape can be for organizations, right, that really amplifies the need to get the right stakeholders engaged in that kind of conversation early within organizations.

Carrie Gardner: Absolutely. And it's the privacy program officials who are able to kind of leverage best practices from privacy by design to think about the design interactions for our build or buy. And so in thinking about being proactive and future proof-- so even although something may not be a requirement at the moment, how can we design the most configurable solution? So if we do need to change our collection or processing capabilities, how can we make the form of it be the most flexible to enable those different types of requirements ahead of time. We're also thinking about differences across users, across groups. So if this a solution where it's collecting user data for marketing, for instance, and there's opt in for that process, how can we ensure that data is being collected and processed in an individualized manner. So that's where really _____ 00:47:13 keying in on the privacy by design practices to ensure flexibility in the solution development lifecycle is very critical here.

Dan Costa: Yeah. And that's a really good example of an opportunity for kind of collaboration between the technologists and the privacy professionals, right, because when you're down at that level of granularity, now we can start having the conversations that make sure the privacy practitioners understand the nuts and bolts of what's happening kind of within how that particular tool is configured, can be configured, or how it got to whatever output its produced, right? That'll ensure that there is the transparency, that there is the explainability that's needed to make those assurances with regards to kind can we or can we not provide these particular guarantees from a privacy perspective using this tool as it is currently configured, or how it could potentially be configured, right? So that is a really good example of kind of how we bridge that gap, right? And it comes through tight collaboration, coordination, and finding kind of that sweet

spot with regards to kind of unpacking the technical underpinnings of how something works versus our expectations for how it should work.

Carrie Gardner: Absolutely. I love how you pointed out the explainability piece. So, for instance, in some circles there is a myth that on their own networks that all of this particular type of machine learning algorithm is a black box. And actually if you talk to the technologists, you talk to the machine, the experts, there's ways to extract out different explainable factors. Some that come to mind are shapely or line value. And so if you have the technologist in the conversation to help identify how can we make something a little bit more explainable, a little bit more privacy centered and protected, then we can build in technical requirements to address those needs while at the same time, giving you flexibility to take advantage of that technology, because we don't want to be in a position where we're just kind of like crossing out a potential solution, that we don't fully understand its capabilities. So I think that's a fantastic example, thinking about the explainability factors and how having a bit more expertise and thinking about what can we do to provide some safeguards on that use.

Dan Costa: Great stuff, Carrie. Let's think about kind of what the research landscape looks like in this space. This might be an opportunity for us to talk about kind of some of the things that we're already doing in this space, particularly kind of the community of interest that we've established with regards to folks that might be kind of working in the area of privacy program development. So Carrie, if you could just get us started with kind of what the research landscape looks like from your perspective right now in the area of kind of privacy and privacy program planning and implementation.

Carrie Gardner: Absolutely. So there's a lot of research out there on the consumer of privacy protections and controls. A lot of that I think spun out of the personalize advertising industry, thinking about how can we make the most-- the best type of ad and targeted ad for consumers. There's a lot of research out there on providing privacy enhancing technologies and notices to users and to consumers to help them make the best decision on whether or not they want to opt in to that data collection _____ 00:51:03. On the organization side, I think we have a lot of room to grow in thinking about the operations, the _____ 00:51:12 themselves that an organization can leverage technically, technical controls, measureative [ph?] controls to build in data protection and privacy requirements at the organization level. And, again, this is where this comes in the picture and kind of giving us an initial framework to work with. But they also have identified challenge areas and thinking about what's next to actually carry out those controls they have. So a few of them come in the form of risk assessments. So that's something that we do here at the Software Engineering Institute is a variety of risk assessments on the system

level or the program level, thinking about how do the controls synchronize together to best carry out and protect an asset, or to protect the organization. So I think we have room to work with in creating an evidence-based assessment methodology on individual systems and thinking about how can we ensure that privacy by design was not only kind of developed and kind of like used during the system development process, but how is it still being protected and respected in application today. And I also think on the program level, using our assets and resources through like the CRR, the cyber risk and resilience assessment, or we have insider threat program evaluation, how can we utilize our knowledge on those types of instruments to develop and design an evidence-based privacy assessment analogue to help organizations best measure where they're at in terms of privacy risk.

Dan Costa: Yeah. I think the measurement piece is certainly something that we're seeing as kind of a-- not necessarily an emerging research need, but one that becomes more amplified as organizations try to adopt some of these kind of privacy risk-based approaches to addressing these concerns within their organizations, right? To quantify that risk, we need to be able to do that in some technology assisted manner, some semi-automated form or fashion, and we've got to be able to trust the math that we're using to address those privacy risks. We've also got to make sure that those systems are instrumented with the censors that can give us data to make those measurements on some kind of near real-time basis, right? So there's a lot of work to do when we're thinking about kind of privacy by design with regards to kind of where we might need to enhance our controls to allow us to make these measures of privacy risk because they'll change. These are dynamic just like a myriad of other risks that organizations experience, right? So it's not necessarily just a new law, or a new policy kind of internal to the organization has been developed that might change a risk landscape, but how a particular business process or security function is being implemented or being practiced that might change your privacy risk exposure. So how can we instrument those processes and the technologies we use to support those processes to allow us to make these kind of dynamic measurements of risk as things change within our organizations. It's a really interesting problem, and certainly lots of more research opportunities out there to try to better articulate kind of where those opportunities for more instrumentation are across these processes.

Carrie Gardner: Yeah. And another research angle I think is really interesting is demonstrating the feasibility of using technologies like AI to automate processes that support privacy risk management. So the second bullet I have there, PII identification categorization, as we've been talking about a variety of different regulatory frameworks, and each of them defines PII a slightly different way. And so if we had that set of applicable frameworks for your organization, can we automatically identify PII across documents based upon attuned natural

language _____ 00:55:51 solution? That's something that I think is a very interesting question. My gut is telling me that's worth studying, evaluating a little bit further, but that's a way we could kind of investigate technologies and potential solutions and help organizations make the right investments for their risk management.

Dan Costa: Carrie, as we look to wrap up here in a few moments, if you could talk a little bit to what we're doing from kind of an outreach and transition perspective with regards to a community of interest that we've established for privacy program professionals, I think that would be a fantastic resource to share with our audience. So could you tell us a little bit more about what the PSIG is and how folks can get engaged in that?

Carrie Gardner: Absolutely. So the PSIG spun out of the Open Source Insider Threat Working Group, or OSIT, and so that's a community of interest that we have been running for many years now. And there's a few different specialty groups. And the newest one that we put forward is the Privacy Special Interest Group. And so this group has individuals from insider risk as well as privacy. And what we're doing in these conversations that we're having monthly is helping develop a better understanding of different technical controls or administrative controls and operational practices that can be used to enhance privacy operations. It is coming from thinking about the intersection of insider risk and privacy risk management. And part of that is to be able to really amplify the need for enhanced sharing between enterprise risk management efforts. So we're starting at thinking about the intersection of insider risk management and privacy risk management, but the conversation is thinking about broader enterprise risk management efforts. How can we leverage existing capabilities and operations to inform and enhance better practices?

Dan Costa: And how can folks get involved in that group, Carrie, if they're interested in joining? And who is it open to?

Carrie Gardner: Yeah. So you can reach out to myself or Ann Connell. We're co-leads of the group. We're actually meeting Friday at 2 p.m. eastern. And so it's open to folks in either an insider risk program or a privacy program. We do have it right now set for industry members. As with our OSIT group, we do kind of have this tailored at industry. Maybe in the future we could to look to open it up further to the public sector as well. But right now, we welcome anyone in an insider risk program or a privacy program, or even if you're interested-- if you're coming from a broader ERM unit. I think that's something-- you probably would find this information also valuable.

Dan Costa: Tremendous. Well, Carrie, this was a lot of fun getting to talk privacy shop with you over this webinar. Lots of great insights from your expertise and certainly as I think we've demonstrated here, lots of lessons to be learned from kind of how privacy programs have kind of been worked into kind of overarching risk management capabilities. And lots more research to be done to help organizations kind of continue to mature their privacy programs, adopting a risk management mindset. And so, Carrie, thanks again for the time, the conversation. Thanks to you all who have been watching, and Shane, I'll hand it back over to you wrap us up here.

Shane McGraw: Great. Dan and Carrie, great discussion today, and thank you very much to both for sharing your expertise in this area. Lastly, as Dan mentioned, we'd like to thank you all for attending today. Upon exiting, please hit the "Like" button below the video window and share the archive if you found value. Also you can subscribe to the SEI's YouTube channel by clicking the SEI seal in the lower right hand corner of your video window. Lastly, join us for our next livestream, which will be April 14th, and our topic will be service level agreements with Matt Markovich and Alan Levine. Registration information will be on the SEI website soon and will be emailed out as well. Any questions from today's event please send to info@sei.cmu.edu. Thanks, everyone. Have a great day.