5 Best Practices for Preventing & Responding to Insider Threat

featuring Randy Trzeciak Interviewed by Eileen Wrubel

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

My name is Eileen Wrubel and I am the tech lead for the Agile in Government Team here at the SEI. With me today is Randy Trzeciak who is the technical manager for the CERT National Insider Threat Center. Today, we are going to talk about the latest edition of CERT's *Common Sense Guide to Mitigating Insider Threats*, which provides current recommendations based on the insider threat team's current research.

Randy, it is nice of you to join us today.

Randy Trzeciak: Thank you.

Eileen: Can you start by telling me a little bit about you and how you got here, how you started working on insider threat?

Randy: I have been at Carnegie Mellon for quite some time, doing a lot of different projects around information security. I started working with computing services, helping them to build security systems around campus. I had come to the SEI to help with a number of areas including building executive information systems in a transition around the 2006 timeframe into the CERT program, which was really focused on information security from an insider threat perspective. So, my background is more of an operational researcher trying to apply that into organizations as we build information security practices and protocols and techniques.

Eileen: Great. For our listeners who might be new to this topic, can you give us a little overview of what do we really mean by insider threat. What might that look like?

Randy: That is a great question. We have been working with organizations for quite some time and trying to address insider threats to organizations. We really start by trying to describe the difference between *insiders* and *insiders who threaten critical assets to organizations*. That is really a clean definition that you need to be able to start with when you are trying to address insider threats.

So, in a context of employees and organizations, we are all *insiders* to our organizations, but we all do not all pose a threat to the critical assets of an organization. What we try to do is really to help organizations to formulate, *who are the individuals that pose a threat to an organization's critical assets?* Starting with that, it is a great foundation from an organization perspective.

When we look at insider threats, it is really focusing on the critical assets of an organization, who could compromise the mission of an organization by impacting the confidentiality, the availability, or integrity of those key information assets within an organization.

Eileen: What is the scope of this problem?

Randy: Well, from an organization standpoint, when we attempt to address insider risk to organizations, the threat posed by insiders—really anyone who has authorized access to the facilities, to the people, to the information or technology—theoretically they do pose a threat to those critical assets. So, recognizing that from a threat standpoint, really all of us potentially could pose a threat. What you need to do is build a security practice around how to identify who is more likely to cause harm to organizations.

We will look at some of the recent surveys that have been done recently. Looking at the CSO [2017 State of] Cybercrime Survey, which we have been participating with for some time now, about 50 percent of organizations experienced at least one malicious insider incident in the previous year, according to the survey.

Eileen: 50 percent. Wow.

Randy: Yes. Pretty significant. And these are malicious insiders who cause harm to organizations.

Eileen: Wow. We have a lot to worry about. Can you tell me about how the *Common Sense Guide* is developed and what is in this newest edition? I understand that there are 20 practices listed, but your blog post focuses on the top five, the most important five.

Randy: That is correct. We are very fortunate to have published this for a number of years. The *Common Sense Guide* is now is in its fifth edition. What we try to do is use an empirical base of actual insider incidents. Since 2001, we have amassed a repository of close to 1,600 incidents

where insiders have caused harm with malicious intent or without malicious intent and tried to build what we think are the ways that those particular insider incidents have evolved over time.

From that what we want to be able to try to do is to help organizations to identify if an individual poses a threat to an organization and what you can do to mitigate that particular threat. Those 20 best practices have evolved around what we think would be effective counter-measures to organizations attempting to mitigate insider threats within an organization.

Now, when you look at the *Common Sense Guide* and the 20 best practices, there are a significant number of those best practices which are information-technology, information-security-specific best practices. But also we recognize the need to make an enterprise-wide risk assessment process to where, we feel it would be very effective to have human resources be involved in insider threat mitigation, physical security, the organization components that are actually doing the threat identification which could include the risk management component of an organization.

If organizations are working with trusted business partners such as contractors, suppliers, anyone in a supply chain, those individuals that you have given authorized access to could potentially threaten an organization's critical assets as well. So, looking at the best practices, we feel there are technical controls, but there are also policy practices and procedures that could be and should be implemented when trying to mitigate insider threats.

Eileen: Randy, one area that we focus on at the SEI is transitioning our work to our stakeholders in the federal government and to the general public. As far as implementing these practices, if I am a technical manager, an HR manager, a CIO, a CTO, what can I do to make sure that efforts to deter insider threat are taken seriously in the organization?

Randy: Well that is a great question. We have been helping organizations across the DOD, the federal government, law enforcement, and industry, trying to implement insider threat mitigation plans within their organizations. In 2011, an executive order came out of the White House mandating organizations that manage, operate, or access classified information to build formal insider threat programs.

So, the DoD has recognized the ability and the need to build insider threat programs for quite some time. Late last year, at the end of the 2016, the NISPOM—the rules and regulations that guide defense contractors—also was modified to require defense contractors to build formal insider threat programs. So, it is very fortuitous that we are actually working with organizations that recognize the need to build these programs.

So, when we first start with the organizations, it is recognizing a threat that exists, recognizing the difference between malicious insiders, the non-malicious insiders, and *how do you build a*

program that will address those threats to the critical assets?, keeping in mind that an organization that cannot fulfill the mission of its organization will not be successful. The threats to those organization's critical assets could be initiated inside the organization or outside, with malicious intent or without malicious intent. So, it really needs to start from an enterprise-wide perspective of getting senior leadership buy in to recognizing the need for a program, have an effective way to communicate the mission and scope of the insider threat program, and ways to implement it, but also finding ways to measure the effectiveness of the mitigation practices, policies, and procedures you are putting in place.

Eileen: OK. Great.

Something I am always fascinated with is the range of topics that your work covers. It hits on social media, workplace violence, and a number of other issues that we do not always think about when we are thinking about cybersecurity.

Can you give us a brief overview of what you are working on, and where you think the state of the research is headed?

Randy: Happy to do it. Again, the foundation of our work is really differentiating the different types of insider incidents. So if you are trying to build a program, a plan that addresses someone who may be stealing the intellectual property of your organization, I would certainly suggest you go to our website and look at the theft of IP, the models, what we build, what the potential risk indicators are. Now someone stealing intellectual property would be different from someone who is defrauding an organization, different from someone who is sabotaging a network or system. That is different from who would be committing espionage against the United States in a DoD or a federal government environment.

So really, building a program to be effective of trying to mitigate an insider from doing something specific is where the program should start. So, when you are building the technical controls that are put in place, there are a number of tools that may be effective, and many times organizations are implementing these tools currently in place. So, data loss prevention, a general category tool that could look for someone taking intellectual property from an organization. Looking at tools such as intrusion detection systems, intrusion prevention systems, using a SIEM tool, a log aggregation tool, to pull all the data together to identify the anomalies of insider threats within the organization.

Recently, newer categories of tools are coming out such as user-activity monitoring, user-behavior analytics, as well as user entity behavior analytics. Really what those tools are looking to do is to bring data together from across the organization, allow a security operations center to configure rules and alerts to alert when certain things are happening, and then we can start

prioritizing some of the alerts that are coming out of these tools that are being implemented within organizations.

Really, the foundation of that is trying to prevent a cyber incident from happening. But recently we have been working with organizations in the DoD and the federal government to try to prevent the physical incidents where insiders could cause harm as well. So it is really the overlap between the cyber and physical.

Recently we have been also working on new areas of research into workplace violence. As you look to build a formal insider threat program identifying someone who may be wanting to harm the organization, whether it be the cyber assets or the physical assets in workplace violence should be part of the scope of the problem as well.

Eileen Wrubel: I would love for us to be able to sit down maybe a couple of months from now, and talk a little bit more about what you have been up to in the intervening timeframe. Thanks so much for taking the time today, I really appreciate it.

Randy: You are welcome.

Eileen: To view a series of blog posts that Randy's team has developed on the 20 practices described in the *Common Sense Guide*, please visit CERT's Insider Threat Blog at insights.sei.cmu.edu/insider-threat. To download the latest edition of the *Common Sense Guide*, please visit our digital library at resources.sei.cmu.edu. You can click on the browse by topics button and then click on insider threat, or type *insider threat* in the search bar. We will include links to all these researches in our transcript.

This podcast is available on the SEI website at sei.cmu.edu/podcasts, Carnegie Mellon University's iTunes U site and the SEI's YouTube channel. As always, if you have any questions, please do not hesitate to email us at info@sei.cmu.edu. Thank you.