Protecting Against Insider Threat
Transcript

Part 1: The Threat

Julia Allen: Welcome to the CERT Podcast Series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org. Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I am a senior researcher at CERT, working on security governance and executive outreach. Today I'm very pleased to introduce Dawn Cappelli, who is responsible for leading CERT's efforts on insider threat, which we'll be discussing today. So, Dawn, it's great to have you here. It's been a while since we've seen each other, and I'm really looking forward to talking with you about insider threat.

Dawn Cappelli: Well, thanks for having me.

Julia Allen: Most organizations, when they think about threat—cyber security or information security threat—think about external threat, think about the hackers and the attackers. What are some leading types of insider threat, and what have you found? Why do you think leaders need to pay attention to it?

Dawn Cappelli: We have studied insider threat since January of 2002, and we started with an insider threat study that we did with the United States Secret Service. So we collected 150 actual insider threat cases and analyzed them extensively. What we found was that the crimes basically fall into three major categories: fraud, theft of information, and what we call insider IT sabotage.

The reason that we think that people need to pay attention to this is that it appears that they are becoming more prevalent. We've done an electronic crime survey for the past three years with the Secret Service and CSO Magazine, and last year, 20% of all electronic crimes were reportedly committed by insiders, according to the survey. This year it was 27%, so it actually has gone up quite a bit.

Julia Allen: So it's either going up or it's certainly being reported more frequently.

Dawn Cappelli: Right. Right. And the target audience for this survey is the CSO subscriber list and the Secret Service Electronic Crimes Task Force members. So we made sure that we got people who know what they're talking about and who have good information for us.

And also, according to this survey, last year 39% of the organizations experienced at least one insider threat. This year that went up to 55%, so over half of all of the organizations have experienced an insider threat. And we define insider threat as deliberate, malicious activity, not accidentally clicking on an infected email attachment.

Julia Allen: Right. Because I think from my observation, most organizations think that once someone works for them or is kind of part of their staff, that there's a level of trust that's established there, so it sounds like clearly what your research and analysis and surveys are revealing is there needs to be a much greater level of diligence paid to folks on the inside, because they have the keys to the kingdom.

Dawn Cappelli: Right, exactly. We started out in our study in collecting information and gathering statistical information on insider threats. Organizations found that to be very valuable, but we were afraid that they were missing the big picture. What we found was that that "trust trap," we call it, is very key. We've worked all along in our research with psychologists, so, you know, we think it's very important that you don't see this as just a technical issue, but you need to understand the psychology of the insiders, the impact of the organizational culture, the impact of policies, practices, technology. Really, unless you understand that whole big picture, you're going to be vulnerable to insider threats.

Julia Allen: Yeah. I can see why it's a very broad-based issue that has a lot of aspects to it that most people probably don't even take into account. So let me ask you, you mentioned the three classifications of insider threat, which I suspect we'll be talking about. But can you give me an example of a case that you've looked at that illustrates kind of the breadth and depth of the threat, or maybe some surprising dimensions of the threat?

Dawn Cappelli: Well, we were fortunate to be able to actually interview some convicted insiders.

Julia Allen: That must have been pretty interesting.

Dawn Cappelli: Oh, yeah, especially the one that was in federal prison at the time.

Julia Allen: Boy, I guess you never thought that your job would be to go interview somebody in prison.

Dawn Cappelli: Right. That was the most exciting day of my career, getting to go into federal prison as a visitor. This one insider that we interviewed, he worked for an investment firm, and he was their star trader. He was a foreign currency trader. And what they found was that over the course of five years he had been losing money, but he had been covering it up, so it looked like he was actually making a lot of money for the bank. And five years later they finally determined that he had actually lost $691 million.

Julia Allen: Oh, my word.

Dawn Cappelli: And had hidden it for five years.

Julia Allen: And it sounds like hidden it particularly well for that length of time.

Dawn Cappelli: Right. Right. And that was a case where we really, without that interview, would not have been able to determine how he did it, because the case file on him was extremely thick, extremely detailed. But they did not really get into, "How did he do this?" So we got to ask him, "What made you think of this? How did you figure out how you could do this?"

Julia Allen: So getting back to your points about the psychology and the culture, and kind of what was in the environment that allowed him to get away with this?

Dawn Cappelli: Right. And with him it was the fact that he was the star, and when anyone even suspected—which they did, they had checks and balances—but whenever someone who was responsible for the checks and balances reported their suspicions, he would go into a tirade and threaten to quit his job. He's the star here, and how dare they question him. And so he intimidated management into ignoring the signs.

Julia Allen: Right. And so it sounds like there was no independent check or balance outside of that kind of behavior that would still examine what he was doing.

Dawn Cappelli: Right. And this is where the psychology comes in, where they let his intimidation and his personality make them deviate from the practices that they had in place.

It was also interesting when I really delved into "how did you do this?" I said, "Did you just accidentally discover a vulnerability in the system? How did you figure out how you could hide this much money?" And he said, "Well, it was easy because I was the programmer of the system."

Julia Allen: Being the trader and the programmer, you know, talk about keys to the kingdom.

Dawn Cappelli: Yes. So when you think of separation of duties, you never think of it in that context, that you build a lot of your role-based access controls, and a lot of your integrity checking and everything, into your systems. And you're relying on those systems to enforce your policies. And if you let one of your end users have access as the programmer, then you're really opening yourself up.

Julia Allen: So in that particular case, a really rigorous and enforced separation of duties might have helped mitigate or close that door to him.

Dawn Cappelli: Right. Right.

Julia Allen: That's really fascinating.

Part 2: Warning Signs

Julia Allen: So you mentioned that he was involved in trading and worked in the financial services sector. Does that tend to be the sector that's most targeted? Are some more targeted than others?

Dawn Cappelli: No. We found that really it goes across all of the sectors. Fraud, of course, is committed quite frequently in the financial sector, but it also can be committed in other sectors where employees are paid by outside to change information. They can steal information in any sector, and in particular the IT sabotage—any sector is vulnerable to that.

Julia Allen: We tend to think of the financial services sector just because we think that's where all the money is. But it sounds like obviously there is gains to be made regardless of what the industry is that you're part of.

Dawn Cappelli: Right, right. Certainly for fraud, that is where the money is, and most of the cases in the banking and finance sector were fraud. But, you know, we had identity theft cases that happened in, for instance, IT companies, where these IT organizations are running the systems for the financial sector, or they're just managing systems that have people's Social Security numbers and personal information in there. So when you think about all of the different kinds of companies that have your Social Security number, really fraud and identity theft can be committed in more sectors than just the financial sector.

Julia Allen: Well, yeah, I think you mentioned that there are three, or you have come up with three categories for the types of insider threat that you've seen. Could you briefly describe those for us, what the different kinds are? And you have mentioned a couple of them.

Dawn Cappelli: Right. The first was fraud, so that was the kind of case that I told you about with the trader. The second is theft of information, theft of confidential information or proprietary information...

Julia Allen: That's where identity theft would come into play.

Dawn Cappelli: Right, right. Identity theft kind of falls into both categories, because they are doing it for financial gain, so there is the fraud element, but they are stealing confidential information. So that would go into both categories. We had information stolen—proprietary company information, new, strategic products that they were developing. Sometimes the insiders took that information. In many of these cases, they were leaving to go to a new job.

Julia Allen: Oh, so they were taking the information with them.

Dawn Cappelli: Right. Either they were taking it because they just didn't realize that there was a problem in doing so, which is kind of interesting, because informally among team members we all said we can see how that would happen. You developed software and it would come in handy in your new job. And if you were going to work for a company that is not a competitor of your company, chances are this happens all the time. But in some of these cases, they were going to work for competitors and they took information with them. And in that case, sometimes the new employer turned them in and said, "You know, I hate to say it, but this person brought this code with them." Other times insiders were disgruntled and they offered to sell the information to a competitor. And, again, interestingly, the competitor often turned in the person to the company, so they sort of watch each other's backs.

Julia Allen: Boy, that is pretty interesting. And then what is the third kind of category?

Dawn Cappelli: The third is IT sabotage, and that's the category that we've really been focusing on in CERT, because first of all, it's the most technical crime. This is the kind that is committed by your system administrators and your DBAs, your privileged, your technical users.

Julia Allen: Your database administrator?

Dawn Cappelli: Right. These are crimes where we've actually gone from just gathering statistical information on this to creating a model of insider IT sabotage. And what our models have shown us is that there are patterns to these crimes, very distinct patterns. Typically, you have some person who has what the psychologists call a personal predisposition. There is something about them that they can't handle things the way other people can.

Julia Allen: And there's a way to actually tell that as you work with people, or maybe even do background checks on them?

Dawn Cappelli: Right. First of all, background checks—we found a large number of these people had a previous arrest history. It was over 30%. But even more than that, it was that they exhibited concerning behaviors at work. So something made them mad. Something upset them. It can range from a new supervisor came in who they didn't get along with, they were denied a promotion, the bonuses were lower than they were supposed to be—so there was a broad range of motivation. But something made them disgruntled.

Julia Allen: Right. So something shows up in their behavior traced to some catalyst or some event.

Dawn Cappelli: Right.

Julia Allen: But you can see that they're not behaving like everyone else is behaving.

Dawn Cappelli: Right. I mean, other people might be disgruntled, too, but they get over it. So there's that initial "everybody's grumbling," but they get over it and this person doesn't. And they continue to exhibit these concerning behaviors, where they're yelling at people, they're late for work, their performance drops. Things like that.

So it starts with these behavioral precursors. And if management can catch it at that point and try and deal with the problem, then hopefully you can head it off at the pass.

Julia Allen: In other words, as a preventive measure.

Dawn Cappelli: Right.

Julia Allen: Right. Or maybe get them into some kind of a counseling or employee assistance program, or ask them to leave.

Dawn Cappelli: Right. Well, okay. Well, let's come back to the asking to leave. But what we found was often those behavioral precursors just go either ignored or just not noticed at all by management. And that's when things escalate and they begin to commit the technical precursors. So these are system administrators or privileged, technical users, and now they go in and they start preparing to attack. They have the idea. They either create backdoor accounts. Some of them downloaded password crackers and cracked passwords for other employee accounts. Some of them created logic bombs and installed them on the system and set them to go off later. So they take those technical preparatory actions.

And what we try to show in our modeling is just this sequencing—that you don't want it to get to this point. But when you do observe those behavioral precursors, you might want to start increasing your technical monitoring of that employee, so you see if they create a backdoor account.

Julia Allen: Based on your analysis, you've kind of got this profile or this sequence of steps, and so if you see one, you want to start looking for the others.

Dawn Cappelli: Right. Right. You need to recognize what could come next and be prepared for it. And the other thing that we have in our model is the impact of sanctions. You talked about asking them to leave. I believe it was 57% of the insiders that committed IT sabotage in our study were former employees. So over half of them were able to come back and attack after they either quit or were terminated.

Julia Allen: Oh, so you are saying they put a lot of these technical measures in place, but didn't access them or enable them until after they were already gone.

Dawn Cappelli: Right. Right. Either they were mad enough that they just wanted to quit and they figured, "Hey, I'm going to come back and get them after I leave." Or they could see the termination was coming—they knew they were in trouble—and so they set up their attack. So they created backdoor accounts. Management didn't know these accounts even existed, and then they can come back in after they're fired. Even if their accounts are disabled, they still have...

Julia Allen: They found another way in to get remote access.

Dawn Cappelli: Right. What we call these is unknown access paths. They create unknown access paths into the system. And that's why it's important to be doing that monitoring, and to have best practices in place, because some of these people—you can't wait until you're ready to fire them to start monitoring and to start doing account audits and employee security awareness training. If you don't have that in place, then by the time you realize you're going to be terminating a system administrator, it's probably too late.

Part 3: Mitigating Insider Threat

Julia Allen: So you've started talking about some of the practices that you've discovered really help mitigate against insider threat. Can you kind of summarize what some of those are for us, and if you have any sense of order or progression, or if I'm a business leader and I can only do a few things to get started, maybe you can give us some idea of which ones to do first and second and third.

Dawn Cappelli: Really, a big one is employee security awareness training, because in the fraud cases, it was amazing to us how many other employees knew that...

Julia Allen: Oh, that something was going on.

Dawn Cappelli: Right, right. They either knew or they suspected. And they just didn't know what to do about it. They don't know who to tell. They don't know if they should tell. Will I be a tattletale?

Julia Allen: Right. The whole whistle-blower mentality.

Dawn Cappelli: So there needs to be some balance between reporting suspicions and going on witch hunts and having people just turning everyone in. But there were so many cases where employees shared their passwords, for instance. They did it because it just made things easier. A lot of times separation of duties is enforced in your systems by role-based access. So if multiple employees share their passwords, it's just much easier. Then I can enter the data and I can use your account to go in and approve of the information and make it official, rather than two people having to be involved.

Julia Allen: Right. But clearly when you're trying to enforce those kinds of practices you want to maintain that role-based separation and have the two people, because that gives you the check and balance. But the question is culturally when folks are just sitting at their desk doing their work, what is it that's going to motivate them to behave in that way?

Dawn Cappelli: Right. And one thing that might motivate them is knowing that if you share your password with your coworkers, and one of those coworkers uses your account to commit fraud or to do anything illegal, when they look at those system logs, it's going to be your account that did the illegal actions, and law enforcement is going to come after you. So if people realize that, I think that they would be much more reluctant to share their passwords, because system logs are right there. They can easily track down who did what.

But it was interesting, in the IT sabotage cases, you have your very technically sophisticated insiders. They know that. And so in many cases they tried to conceal their activity or frame someone else for their activity by modifying those system logs. So that brings up another important point. It's very important to protect your system logs.

Julia Allen: That'll be another practice.

Dawn Cappelli: Right.

Julia Allen: Employee awareness, protect your system logs.

Dawn Cappelli: Right. We had an insider who just downloaded a logic bomb from the Internet, and then went into the system logs and changed it so that it looked like his supervisor had done it—just changed who downloaded it to his supervisor's user ID. Then went to his supervisor's boss and said, "Hey, you know, I hate to say this, but my boss downloaded a logic bomb. I was looking through the logs and I saw this. It didn't go off, but he downloaded it." And the supervisor got fired. It was only after he hired an external forensics firm to come in, he was able to prove that he didn't do it. But that wasn't the only case where they framed someone else by using those logs.

Julia Allen: Right. But again, if the system's logs weren't there, and if they weren't trusted—in other words, if they weren't created in a way where you can append only, and you can't modify the system logs—then he would have had nothing to back up his claim.

Dawn Cappelli: Right, right.

Julia Allen: So what are a couple of other practices that you recommend? I know recently you've published a Common Sense Guide for best practice for insider threat. So what are some of the other ones from that?

Dawn Cappelli: A really important one is account management practices. It was interesting in our e-crime survey that we asked, "What are some practices that you have in place in your organization for security?" And one of the top practices was account management. It was 92%, I believe. So we thought, "Oh, well, that's really good." But then when we looked at how many organizations actually do periodic account audits, it was like 42% or 48%.

Julia Allen: But they put the practice in place, but they don't monitor, review, and necessarily enforce the practice.

Dawn Cappelli: Right. So we saw a big gap between just having a policy and actually having the practice in place to enforce it. And so many of these insiders used someone else's account, and so many of them created backdoor accounts, that it really is important that organizations review their accounts and make sure that they are legitimate accounts, that accounts that are no longer needed are disabled.

Julia Allen: And when people leave that their access is removed.

Dawn Cappelli: Right. Right. One insider, he saw it coming. He knew he was going to be terminated. And he created VPN accounts for...

Julia Allen: Virtual private network.

Dawn Cappelli: Right. For his supervisor, the VP of Sales, and the CFO. So he created three VPN accounts for legitimate employees, but he didn't tell them that he'd created them.

Julia Allen: So that he could use them after he left.

Dawn Cappelli: So he was the only one that knew the passwords for these accounts. He was the only one that knew that they weren't legitimate. And then after he got fired, he went in for two weeks and used those accounts to go in and set up his attack. And even if they had been monitoring, they wouldn't have known that that was illegitimate activity because it looked like legitimate accounts.

So that just illustrates how complex some of these attacks are, and why it's important to understand the psychological issues, as well as the technical, because you really need to approach it from both ends. You need to try and stop the attack from happening to begin with.

Julia Allen: You mentioned logic bombs and backdoors and other software elements that are in the more technically based attacks. Could you just say a little bit about how do you detect those? How do you know that you've got that kind of software—rogue software—running around your system?

Dawn Cappelli: With the logic bombs, if they had characterization processes in place where they actually looked at new software, new files that were released onto their production systems...

Julia Allen: In other words, you can actually track how your configuration has changed and then examine those changes.

Dawn Cappelli: Right, exactly. One thing that we emphasize in our best practice guide is that you need to do enterprise-wide risk assessments. You need to look at, "What do I really need to protect?" You can't fully protect every single thing on every single system.

Julia Allen: It's not cost effective.

Dawn Cappelli: Right. If you know what your really critical assets are, then you can put processes and technology into place to really protect those. So if you have this software running that tells you, "Here are all the files that changed in the past week," you can look and see, what were the changes? Who changed them? Were they legitimate changes?

Julia Allen: Does anything look suspicious?

Dawn Cappelli: Right. The one insider, he actually changed the log file rotator script that comes right out of the box with Solaris. He went into there and changed that script so that whenever a certain log file reached a certain size, instead of rotating the log file out, it set off a logic bomb to wipe out their entire system. He went in and just modified that script when he found out that he was being terminated. So that just goes to show if they had been looking, they may have looked and said, "Well, why would anyone modify the log file rotator script? Why would they do that? What did they do to it?" And they could have noticed. There was one insider who planted a logic bomb, quit, and it went off six months later.

Julia Allen: Right. So there was a long period of time where you probably wouldn't even associate it with that individual.

Dawn Cappelli: Right. And that's why you have to have best practices in place all the time.

Julia Allen: So you've got clearly a very complex issue. It's got people, process, and technology aspects to it. We're learning more about it as time goes on. So if I were running an organization and you've raised my awareness that I need to take some action, what might be the first step I would take to start to address insider threat?

Dawn Cappelli: I would recommend that they go to our insider threat webpage on the CERT website. We have all of our research there. They can read about that. We're starting to offer training. We're actually putting together an interactive virtual training experience now, where it's almost like a video game, where you play the manager against the insider, and you see if you can detect them, prevent them from attacking.

Julia Allen: When do you think that might be available? That sounds really interesting.

Dawn Cappelli: We're doing a proof of concept which will be done by May of 2007.

Julia Allen: Excellent. And we can keep up to date on your portal on the CERT website?

Dawn Cappelli: Right. But we have a lot of resources there. We have the best practices guide. We have our research. We have information about the modeling. And the modeling is really an interesting thing to look at, because that big picture is very important.

Julia Allen: So it sounds like you're saying, first get yourself educated and better informed about the problem. And then think about what aspects of that problem might be germane to your particular organization, your employee base.

Dawn Cappelli: Right. And I think the main thing is to realize that it's not just a technical issue, and it's not just a human resources issue. All of the managers in an organization need to realize how this works and how they're vulnerable, and how they need to work together to prevent this from happening.

Julia Allen: Well, Dawn, I so appreciate your time today. And I think you've given us a lot to think about, and I'm just hoping that as the insider threat work continues to evolve we'll get a chance to talk again.

Dawn Cappelli: Okay. Thank you.

Julia Allen: You're welcome.