Mitigating Insider Threat: New and Improved Practices
Transcript

Part 1: Analyzing Real-Life Cases; Assessing Risk & Raising Awareness

Julia Allen: Welcome to CERT's 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'm a senior researcher at CERT, working on operational resilience and software assurance. Today I'm pleased to welcome Dawn Cappelli, Randy Trzeciak, and Andy Moore, all members of CERT's Threat and Incident Management Team. The last podcast I did with Dawn dealt with addressing insider threat during the software development life cycle. Today the three of us will be talking about the team's latest work in updating their best practices for mitigating insider threat, and some new initiatives, a new insider threat workshop, and threat assessment. So let me first welcome each of you so our listeners will recognize your voices. So welcome Dawn, glad to have you.

Dawn Cappelli: Thanks Julia.

Julia Allen: And Randy, great to have you today.

Randy Trzeciak: It's great to be here. Thank you.

Julia Allen: Andy, thanks for joining us.

Andy Moore: Hi Julia, thanks.

Julia Allen: Okay, so we'll get the ball rolling with Dawn. Dawn, I know we've talked about this before in some of our other podcasts, but I think it would be helpful for our listeners to refresh on your definition, your team's definition, of an insider. So why don't we start there?

Dawn Cappelli: Okay. And we actually have revised our definition recently. Our definition of a malicious insider is a current, or former, employee, contractor or business partner. We've recently added the business partner aspect of that to the definition because of recent trends that we're seeing.

So it's current or former employee, contractor, or business partner who has, or had, authorized access to your network, your systems, your data, and intentionally misused that access. So this is not looking at accidental data leakage. Although we would like to, we have not looked at that yet. So this is intentional misuse of your systems, data or network, and then what the negative consequences to the confidentiality, integrity, or availability of your information or your systems.

What we are going to be talking about today does not include espionage involving national security information.

Julia Allen: Okay, well that's real helpful. And yes, I know the extent to which organizations are working so much with outside parties and partners – I think the business partner addition, obviously coming from your cases, is really a helpful one.

So let's talk a little bit about the cases. I know that all of your work is very well grounded in analyzing actual insider cases. So how many cases have you now analyzed, and over what period of time, and are there some ways that you've categorized these?

Dawn Cappelli: Yes, at this point we have 282 cases in our database. Those span the period from 1996 through the present. And we've looked at them and categorized them by the patterns of how these cases evolve over time. And so we've categorized them into three categories.

The first is sabotage. These are cases in which the insider wants to cause harm to the organization or to a person. So they wipe out data, they bring down systems, disrupt operations. And we have 101 cases of sabotage.

The next category is theft of intellectual property. This is where an insider steals trade secrets, business plans, strategic plans – some kind of intellectual property owned by the organization. And we have 40 of those cases.

And the third category is what we call theft or modification for financial gain. So this is where employees go in and they steal personally identifiable information, credit card information, some kind of information that they then take and they sell; or they modify information, in databases typically, for financial gain. Often they are actually paid from an outsider to do that. And we have 106 of those cases.

We also have 41 cases which either don't fall into one of those three. They're miscellaneous or we don't have enough information on them yet to really know for sure. And in addition some of the cases span multiple categories.

Julia Allen: Boy, that's quite an archive of cases to draw from, and I know you, I'm sure you keep getting new ones all the time.

Dawn Cappelli: Yes, we have students constantly, that's what they do is search for new cases.

Julia Allen: Okay, well let's turn our attention to some of the practices from your latest guide on Preventing and Detecting Insider Threats. That documentation, which we'll refer to in the show notes, comprises 16 practices. We're going to talk about a few of them today; the ones that come from your latest research and build a foundation for the others.

So Randy, why don't you start us off? We'll talk about the first practice. It's called *Consider threats from insiders and business partners when you're doing an enterprise-wide risk assessment*. So tell us a little bit about that practice.

Randy Trzeciak: Sure. So unfortunately, at least in the cases that we've seen, organizations sometimes fail to recognize or include individuals who are outside their physical organization – business partners, consultants, organizations they collaborate with or partner with or otherwise associate with. And they tend to draw the boundary a little too narrow when considering insiders. If you are working with business partners, collaborators, contractors, and subcontractors, and they are having full access to your critical data, we need to consider those individuals when assessing the risk posed to your organization.

Obviously organizations are increasingly outsourcing their critical business functions: obviously the management of data; securing the critical data; organizations that provide backups for organizations. So as a result we're granting people who are not full-time employees of organizations full access to your critical data, your processes, your information, and information systems. And traditionally, this was always provided to just individuals in your organizations.

So to highlight this, we certainly like to give case examples, actual cases that occurred. And in a recent case that we studied by our team – a consumer data organization. They were responsible for accepting data from organizations such as banks, phone companies, and credit card companies. And what they would do is take data from them and provide marketing information in return.

Now this consumer data organization actually subcontracted with a data mining company. And what they basically did was take information from these organizations, such as customer information, Social Security number, date of birth, gender, income, occupation – and it's certainly sensitive information – and provide marketing information back to those phone companies, banks, and credit card companies.

Now this data mining organization had a system administrator working for them, accessing the data owned by the customer information but which is managed by the consumer data organization. What he was able to do was to find an unprotected file with an encrypted password on the consumer data organization's server and actually run a password cracker to obtain the passwords for all of the customer databases managed by the consumer data organizations. And what he did was download millions of records onto removable media and then solicited it for sale on the Internet.

So we like to use this as an example to raise awareness of the threat to the information, which is outside of the control of the organization. So if organizations are contracting or partnering or asking other organizations to manage the data, maybe to make sure that security is written into the contracting agreements. And require the same level of security as if it was managed by the organization.

Julia Allen: That really makes good sense because I've been doing some work in the whole cloud services, cloud computing arena. And a lot of the same issues arise when

you really lose control of who owns the data, where the data's being passed to, who has access to it. And that really isn't totally under your control, right?

Randy Trzeciak: Absolutely. Yes, we certainly – we certainly, say from an organization standpoint, know who has access to your data. And then if – for example, in another case, a final, just very quick case – if we have contractors or subcontractors accessing your systems or your organization, make sure that you have written into your agreement when those contractors leave that organization that you're immediately notified so you can disable electronic and physical access as well.

Just quickly, an example of a contractor who did provide some IT support to a power and electric facility. They suspended an employee on Friday but didn't notify the organization immediately. What this individual did was come in on a Sunday night, access systems, physical location, and actually hit an emergency power off button, shutting down some of the critical computer systems, obviously causing a disruption in service.

So certainly if we have access, and that access is disabled from your contractors or subcontractors, make sure that you're automatically or immediately notified so you can disable electronic and physical access as well.

Julia Allen: Well Andy, let's give you a crack at this. We all know the importance of regular security awareness training even if we don't always do it. So what in your practice development do you find to be some of the unique dimensions of security awareness training for dealing with insider threat?

Andy Moore: That's a good question Julia. There definitely are unique dimensions. And a point that we often start off with, regarding security awareness, is to make people realize, employees realize, that their preconceived notions about insider threat may be inaccurate. Sometimes we call these 'myth busters.' Things like ages range from late teens to retirement; so it spreads the whole range. It includes both men and women. And it includes stereotypical introverted loners but also aggressive, high performers and extroverted star players. So it pretty much is all over the map. And generally what we try to emphasize is that security awareness training should emphasize identification of the insiders by their behavior rather than stereotypical characteristics or profiles.

We describe many of these things in the Common Sense Guidelines that we put out that describes the best practices. Many of the cases include insiders that, for instance, made threats against the organization or bragged about damage that the insider could do. Also there was at times excessive or uncharacteristic interest in information outside the insider's domain, and this – so these things are observable within the organization. They're behavioral in nature and can indicate a heightened risk that, a heightened risk of insider attack that the organization can notice.

Julia Allen: So what do you recommend if someone observes some of these kinds of behaviors? Let's say they've been through an awareness training program and they're

now more sensitized to or attuned to some of the behaviors that you've seen come out of actual cases. What do you advise people to do?

Andy Moore: Right. So we'll talk a little bit later in the conversation about insider incident response. And the idea is that managers need to be aware of these things, and to monitor them, to document them, and to communicate them with other players in an organization, for instance Human Resources. And working together with those other departments, they can decide what to do about those and when to escalate them into something that may be a serious problem. Particularly if these things are happening in advance of the resignation or termination of the insider, they can be more serious. So I think we'll maybe talk about that a little bit later too.

Julia Allen: Okay, well that'll be great. I appreciate that insight.

Part 2: Least Privilege & Separation of Duties; Password & Account Management

Julia Allen: Dawn, over to you. I know in your practices, numbers 7 and 8 in particular, they concentrate on password management, account management, separation of duties, least privilege; a lot of the authentication/authorization practices. When it comes to insider threat, what can go wrong if these aren't well considered?

Dawn Cappelli: Well let's start with least privilege. We found in our research that insiders tend to steal what they have access to. So whether you're stealing customer information, personally identifiable information, or intellectual property, people typically don't have to go beyond what they have authorized access to. But sometimes they have excessive privileges, so they have access to much more than they really should, and that's where least privilege comes in. We have a case, for instance, where a salesman was able to steal source code for a new product being developed. There's no reason why a salesman really should need access to source code that's not even out in production yet.

So it's important that organizations think about that. And it is very difficult to maintain, because people move from project to project, they transfer, they temporarily help out on things. But we've found it's just very important that people, managers, keep a good handle on who has access to what.

Secondly, separation of duties. Traditionally that's thought of, as far as systems, where you need one person to make a change to data and another person to approve that change. We've found that in some of these cases, there were no technical controls to enforce that. So although separation of duties was built into business processes and people were trained as to their roles, it wasn't technically enforced or it wasn't technically enforced correctly.

We also have found that system administrators need to have separation of duties built into their functions. They typically have – obviously system administrators have extreme power on the system but a lot of times they have excessive power. It's worth

organizations thinking about how can we separate the duties here? Do we need to give every sys admin access to every server or can we somehow separate those?

We had one system administrator who was demoted from a senior system administrator to a junior system administrator, which meant that he should've only had access to a single server. But there was no technical control over that. And so he was able to plant a logic bomb that would've wiped out everything on all of their servers. He also was able to modify all of the system logs to cover up his tracks and to actually frame his supervisor for the act.

As far as account management, most of the sabotage cases happen after termination. And they, the insiders, used what we call unknown access paths. These are paths that they create before they leave that give them a way back into the system. Often they use shared accounts because it's very difficult for organizations to keep track of all of their shared accounts. Who has the passwords? There's sys admin accounts, DBA (database administrator) accounts, test accounts, training accounts. And it's often very difficult to just figure out who has access to each of those accounts. But it's very important, and it's important to track what are all of those accounts.

We also have cases where many of these system administrators created backdoor accounts. So they deliberately created an account that looked like a legitimate account but provided them remote access after termination.

And finally password management. We saw users share passwords to get around separation of duties. So it just made their job easier. Instead of me entering something and someone else approving it, if we share our passwords I can enter it and approve it, you can enter yours and approve it, and we can be much more efficient. They don't really realize that that's a very dangerous thing to do and what the consequences can be.

And just one last thing: weak passwords. We have a fair number of cases where system administrators ran password crackers and were able to obtain passwords for other users' accounts. And then that provided their unknown access path to get back into the system following termination.

Julia Allen: I'm kind of taken by some of the earlier remarks – this whole concentration on both current and former employees or current and former users who had access. And I notice you talk about that a lot in terms of account management, that some of the issues that come up happen after people leave the organization. So it just strikes me that organizations don't need to just worry about the folks that are currently onboard but everybody who's ever had access, right?

Dawn Cappelli: Right. And perhaps in a future podcast we could talk about that. Because we have very specific information on who commits each of the types of crimes that we've looked at – current versus former – as well what type of employee and how they do it.

Julia Allen: Well that would make a great topic for the future. I'll take you up on that.

So Randy, building on Dawn's previous response, she introduced a little bit the extra caution that needs to be taken with folks with high privilege, like system administrators and other technical or privileged uses. So what are some of the other nuances in this practice area?

Randy Trzeciak: Sure. So what Dawn went through is lots of examples where system administrators exploited the access they had to commit their crimes. Based upon the statistics that we have in our database, the cases that we've collected, the majority of insiders who committed sabotage – and over half of those who stole confidential or proprietary information – held some type of technical position.

So what we like to challenge organizations to do is to try to institute separation of duties or a two-person rule into their IT operations as well. Many organizations see the need to put a separation of duties or a two-person rule into their business processes but they fail to recognize the advantage that they could have in an organization by implementing those in their IT operations as well.

Some of the cases that we've seen, the technical methods that they use to carry out, to conceal their malicious activity, include: writing or downloading of scripts or programs; the logic bombs that they would deploy prior to leaving an organization or after leaving the organization to commit sabotage; the creation of backdoor accounts that Dawn talked about; the accounts that aren't known to the organization so they can't successfully disable them when an individual leaves; the installation of remote administration tools, system administration tools.

Also we saw lots of cases of modification of the system logs. We saw examples where system administrators, when they carried out their sabotage they were able to install malicious code. But then they were able to go through and modify the system logs to either destroy the system logs to conceal their activity or actually frame another individual in the organization for the crime that they had actually committed.

So again, we try to challenge organizations to implement those separations of duties, two-person rules, to make sure that there isn't one sole administrator who is able to release modifications to critical systems, or your networks or applications, and even your data itself.

So in just one very quick case example, we had an insider who was a system administrator. He actually quit his job with an IT telecommunications and internet service provider but didn't provide any advance notice that he'd be leaving the organization. The organization refused to pay for the final couple of days of employment for this individual. And what this individual did was he changed the system administrator passwords until the organization paid him for his last few days at work. Obviously without those administrator passwords, the staff were locked out of all the administrative functions in the organizations. And actually in looking at the forensics, they actually showed that the insider accessed email, he modified systems to prevent individual access, accessed key system files, and modified key system files.

So certainly, if it is possible in an organization, we certainly challenge them to not have a single system administration for all of your administration in your organization. Put at least two people in system administrator functions so that we do have the separation of duties and the two-person rule to ensure that any changes to critical system files or data is at least reviewed and hopefully authorized by another individual in your organization.

Julia Allen: Okay thanks. Well that certainly makes good sense. Two-person rule is used in a lot of business processes. So it seems to make great sense to apply it here.

Part 3: Logging, Monitoring, & Auditing; Incident Response

Julia Allen: We have two more practices we're going to talk about before we come to our close. So Andy, let's talk a little bit about logging, monitoring, and auditing. We're always barraged with tons of data to take a look at. But how can selected use of those kind of file structures and results lead us to some early discovery and investigation of some suspicious insider actions? How can you use those resources?

Andy Moore: Right. So if you have those good account and password management practices that Dawn talked about previously in place, users can be held accountable for their actions through the logging monitoring, and auditing.

And in terms of sabotage, Dawn also talked about some of the technical precursors that we saw in cases: things like the creation and use of backdoor accounts; download installation; and testing of malicious or unauthorized code. These sorts of things can – are often done earlier on in the cycle and can be detected by organizations using existing tools that are on the market.

In terms of fraud, on the other hand, it's a bit more difficult. These were generally long, ongoing schemes. And many continued for more than a year, and most insiders were – most of these crimes were ongoing or frequent in nature over that period beforehand.

The reason that these are particularly difficult to detect is that these insiders were in relatively low level positions. They weren't technical insiders and so many of their acts were not technical. They were committing these crimes while they were at work using their authorized access. So it's very difficult to distinguish these from authorized acts that they might engage in.

So in the fraud case, it's more the behavioral monitoring that might catch these type of crimes. In the theft of IP (intellectual property) case, they have a very different signature. These types of crimes went on for a shorter period of time. They were generally quick thefts upon resignation. About two-thirds of the cases involved theft within one month of resignation. And some of these were very large downloads and involved information outside of the insider's immediate domain of responsibility.

So this provides a window of opportunity for organizations. We had one case where a research chemist – the four months before he resigned or through the period of four months that he resigned – he accessed 116,000 PDF files and downloaded 22,000 abstracts from the server, from the organization's server that maintained many of the trade secrets for the organization.

So again this is a window of opportunity for the organization and provides a specific signature that they can look at, right before resignation, to detect if they are at heightened risk of theft of intellectual property.

Julia Allen: So you're suggesting based on the case data that you've looked at, that there, as you said, there are signatures or profiles or time windows where organizations might be able to put in specific, either evaluations of their current logs or maybe some extra monitoring approaches around that profile. Am I hearing you correctly?

Andy Moore: That's exactly right. So in the case of theft of IP at least, this would be a good point to check with at the termination exit procedures. Making sure that if somebody's leaving the organization, you might want to look at those logs to see whether you see any of those red flags that I've discussed – either the large downloads or accessing information outside where they shouldn't typically be concerned with.

Dawn Cappelli: Yes and Julia what we try to tell people is we know you can't look at everything everyone does. That's just not practical. But if you understand the patterns to look for, and when to look for them, as long as you're proactively collecting the information, then you'll know what to look for when you see the suspicious patterns arising.

Julia Allen: Excellent. Well Randy, why don't you help us wrap up the practice part of our discussion? Andy alluded a little bit to incident response, and we know that it's proven practice to have a good incident response plan and process in place well before you need it. So why is this particularly critical for insider threat?

Randy Trzeciak: One of the things that we've seen over the period of time we've been doing studies on the insider threat is that there seems to be a common misconception from organizations regarding insider threat – that it's a problem that can be solved solely by information security or information technology and implementing technical controls alone. At least in terms of the research that we've done, we've seen that this is not the case.

What we try to do in our presentations and raising awareness is that in order to prevent insider attacks or to detect them early enough, or to minimize the impact if we're detecting them early enough, what we're saying is that organizations should involve IT obviously. They should implement technical controls. They should have information security be involved. But also to involve human resources, your legal department, your managers that Andy talked about, physical security, and data

owners. And communication obviously between these departments will be essential to identify individuals who may be more at risk of committing these types of crimes.

We know that organizations realize the challenge that it's almost impossible, as Dawn said, to audit everything that an individual does. But if you can observe and communicate some of the potential technical and non-technical indicators of this activity, hopefully we can identify, or organizations can identify, individuals who may be more at risk of committing these types of crimes; the patterns that Dawn talked about.

And certainly it's essential that we involve Human Resources and Legal just to make sure that the increased scrutiny that we're placing on individuals, the increased auditing that we're doing, that it conforms to the organization's policies; any state and local laws as well. Again, we don't want to come across as profiling individuals. But if we can identify these patterns of behavior that may indicate a higher degree of risk, that certainly is something that we can more target in terms of the online actions that Andy had talked about.

And then finally, we certainly recommend getting law enforcement involved as soon as possible when investigating and prosecuting these types of crimes. In a recent crime survey that we conducted – CERT, the Secret Service, Microsoft, and CSO Magazine – one stat that we find interesting is that 70% of organizations that experienced an electronic crime in the year 2007 that was committed by an individual inside the organization, an insider, those organizations handled that internally without legal action or involving law enforcement.

And what we speculate is that to avoid some of the negative media attention that when these inside crimes occur, organizations tend to not involve law enforcement. They tend to let the individuals go, terminate their employment, but they don't involve law enforcement. And again, we're speculating that that may be to try to head off some of the negative media attention.

So what we suggest is certainly involve all parts of your organization, increased communication across the departments, and involve law enforcement as soon as possible to utilize their resources to investigate and prosecute the crimes.

Julia Allen: Excellent. Do you find Randy, are there particular like steering group structures or incident response team structures that seem to work well for bringing all these parties together? Because they all have different interests across the organization. So how do you actually get them into a structure where they can have the kind of interaction that you're recommending?

Dawn Cappelli: Actually Julia we just started working with organizations on that. And we just started offering an insider threat workshop and an assessment service to organizations. And we find that that is really helping to get that message across. And so we're just starting down that road now of working with organizations to put that kind of structure together.

Julia Allen: Okay, well Dawn you started us down this path as we come to our close. Could you tell us a little bit about some of your new offerings, the insider threat risk assessment and your insider threat workshop?

Dawn Cappelli: Sure. The assessment was created because, it was at the request of people out there. We would give presentations and their feedback was, "Can't you pool all of your knowledge into a list for us? Just give us one nice list that we can check off."

And what we found – we did that, we tried. We took every single case in our database and we looked at the cases for what we call issues of concern. And those include technical issues, business process, legal, HR, management, all of the different kinds of issues that we saw that enabled that insider to carry out the attack. And we tried to pool that together into a checklist.

But what we found was it's really the details of the cases that organizations need to consider. If we put a checklist out that said, "would you detect a logic bomb?" They might check that off, not realizing all of the very detailed, sneaky ways that these logic bombs can be planted. It's not going to be called logicbomb.exe.

So what we did was we created this assessment. And we now go into an organization, we spend three days with them, and we walk through six workbooks. And the workbooks cover all of the different issues of concern that we saw in the cases. Really 75% of the assessment covers technical issues. But we also meet with HR, managers, what we call data owners, legal, and physical security, in addition to IT and information security and software engineering. What they get out of that is a report of findings. For each finding we list the prevalence of that issue in our cases and suggested countermeasures.

So we've done, we've done two of these assessments so far and we have three more that are scheduled. And it's really working out well to help organizations identify issues of concern and then to prioritize those in light of a larger risk management strategy.

Julia Allen: Right, because I would think the results of this type of risk assessment could potentially, or should potentially, integrate with other security risk assessments, other organizational risk assessments. In other words, you want to try and help them make this part of their normal risk management, risk assessment strategy enterprise wide, right?

Dawn Cappelli: Yes exactly. We can identify findings. We can identify prevalence in the cases. But it's up to the organization to really make the assessment of how does that apply to my organization? What risk does that pose? And what is the relative priority compared to the other risks that we need to deal with?

Julia Allen: And did you want to say a little bit about the insider threat workshop?

Dawn Cappelli: Yes. We also created a workshop recently. Our goal is that participants in the workshop come and then leave with actionable steps, that they can actually put into place to better manage the risk of insider threat in their organization.

So it's a two-day workshop. It pools together everything that we've done for seven-and-a-half years in insider threat. It consists of presentations and interactive exercises. And we look at all of the kinds of issues that we've talked about today: technical, organizational, personnel, security, process. We also pull in portions of the insider threat assessment into the exercises.

What we found after our first public offering was that a few of the organizations that participated now would like us to come on site and do the exact same workshop. But do it at their organization so they can bring in HR and legal and managers and IT and risk officers. And really have that big picture point of view come across to all of the participants in their organization, so that they can go down that path of really incident response planning for insider threat.

Julia Allen: Okay. Well I know that we've barely scratched the surface on this very rich and well researched topic. So Dawn, where can our listeners learn more about everything we've talked about today?

Dawn Cappelli: We have an insider threat website and that is at www.cert.org/insider_threat.

Julia Allen: Okay, well listen Dawn, I thank you, Randy, and Andy for your time and your expertise today for this foundational work that I know has been of great value to all the organizations that you work with. I know your presentations tend to be standing room only so I'm glad we had an opportunity to capture some of your great recommendations today. So thanks everyone.

Randy Trzeciak: Thank you.

Andy Moore: Thank you Julia.

Dawn Cappelli: Thanks Julia.