Mitigating Insider Threat: New and Improved Practices Fourth Edition
Transcript

Part 1: Over 370 Cases Analyzed to Identify Practices

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 principal researcher at CERT working on operational resilience. Today I'm very pleased to welcome George Silowash and Lori Flynn. They are members of CERT's Insider Threat Center.

And today George, Lori and I will be discussing the fourth edition of their team's Common Sense Guide to Mitigating Insider Threats. The guide describes 19 best practices for mitigating insider threat and for our listeners' benefit as background, we have posted several podcasts on insider threat-related topics including prior versions of the Common Sense Guide, which you are welcome to listen to as interest permits.

So with no further ado, welcome George.

George Silowash: Thanks, Julia; it's a pleasure to be here today to discuss the Common Sense Guide.

Julia Allen: Great. And Lori, we're also very glad to have you on the podcast series today. Welcome.

Lori Flynn: Thank you. Great to be here.

Julia Allen: So George, why don't you get us started? I have a few stage setting questions for you. I know we've talked about insider threat before, as I said, on the podcast series. But I think for our listeners' benefit who are perhaps new to the topic, it would be helpful to refresh on CERT's definition of a "malicious insider" if you would be so kind.

George Silowash: Sure. CERT defines an insider as a current or former employee, contractor, and even business partner who has or had access to an organization's system, network, or data.

The insider has intentionally exceeded or used that access in a manner that typically negatively affected the confidentiality, integrity, or the availability of the organization's information or information system.

Julia Allen: So it's someone who has had access in the past, may still have access, or may have left the organization. Is that correct?

George Silowash: Yes. So sometimes an insider may leave the organization. They either may be terminated or just choose to go on to other employment and either the organization neglects to disable their access or they are unaware of a backdoor into the organization.

Copyright 2013 by Carnegie Mellon University

Julia Allen: Great, thank you. So, Lori, one of the things that I love about this body of work is that I know that it's based on having analyzed hundreds of cases and that your best practices derive from that analysis.

So could you say a little bit about how many cases you've analyzed to date and how these are categorized? It will help give our listeners an idea of the sources of data from which the practices derived.

Lori Flynn: Yes, the work is empirically based. We've analyzed more than 700 insider threat cases. We categorize them in five ways: as intellectual property or IP theft, fraud, IT sabotage, espionage -- and everything that doesn't fit into those categories we call miscellaneous.

The top six infrastructure sectors for the categories are: banking and finance, IT, healthcare and public health. Two of the categories are government: federal is one and state/local is the other, and commercial facilities. And we've analyzed a total of 371 cases for this edition of the Common Sense Guide. We don't include discussion or analysis of our espionage cases. And all of the 371 cases are adjudicated, which means that in a court of law the insider was found guilty.

Julia Allen: I've always been interested in that aspect of it, the fact that you select cases and then you ensure that the cases have been adjudicated; the insider has been brought to justice.

It seems to me those kinds of cases are really hard to find, aren't they? Or do you now have established trust sources that allow you to really track when a new insider threat case is ready for your analysis?

Lori Flynn: Well we have a process where coders monitor media sources for new insider threat cases. And additionally we get some of our cases from organizations, law enforcement organizations like the U.S. Secret Service and FBI who identify new cases that we wouldn't necessarily have heard of through the media sources.

Some of our cases are brought to our attention by businesses who again don't necessarily report their cases to the media but do want to get the benefit of our insight into insider threats and also to give us information to draw new analyses.

George Silowash: Lori, you make a very good point there too. A lot of our cases that we find out about come from media sources and a lot of times organizations just don't want to report about an insider that might have compromised the organization. I mean who wants to actually admit that something happened to their organization and it could negatively affect them either financially or other means? So this is another big challenge when it comes to collecting data about cases as well.

Lori Flynn: That brings to mind the U.S. Secret Service and CERT and various other organizations put together an annual survey about insider threat. We found, according to our survey results, about 76 percent of insider threat cases are not reported to law enforcement or media.

They’re kept in-house for reasons such as an organization not having enough proof to feel that it's worth it to try the case in a court of law. There's too much risk of losing. And also there’s a lot of concern about bad media exposure.

George Silowash: Sure a lot of organizations too just choose to handle the incident internally either terminate the employee or through other some administrative action against that employee. So often times it might not even raise to the level where it's actually reported out to news sources or anything like that.

Julia Allen: Right. So I think the important point to make for our conversation today is you have many cases that you analyze but the ones on which the Common Sense Guide is based have been adjudicated, correct?

George Silowash: Yes.

Part 2: What's New in v4; Cloud Service Agreements

Julia Allen: Okay. So George, let's talk a little bit more about the structure of this new guide and what's new about it and then what we're going to do is get into a few of the new practices.

So could you summarize some of the key differences and improvements that are reflected in this guide compared to the third edition which was published in January of 2009?

George Silowash: Sure I'd be happy to. Actually the Common Sense Guide has undergone a number of changes and enhancements since the third version. For starters we've analyzed more cases, which have allowed us to update the guide to include information about what we're seeing across various types of organizations.

This has also helped us to develop four new best practices. We've refreshed the existing 15 best practices and actually folded one of the other practices into others -- so that would be the software development process that was folded in amongst the other ones that are in the guide.

We also included one or more case examples in each best practice from our database where it was possible. Another feature of version four of the guide is that it addresses a range of roles across an organization. For example we talk about HR, legal, physical security, data owners, information technology, and even information assurance and software engineering.

The Common Sense Guide has actually been I think made easier to use by including a chart at the top that basically tells you which area of the organization that practice is addressing. It's just like a little check box across the top. And we also include appendixes in the document that are tailored to those specific roles too.

One of the things we also did to increase the usability of the guide was to include a "Quick Wins and High Impact Solution" section for each of the best practices. They're a list of suggested quick wins for jumpstarting your organization's insider threat program. They're also tailored to large and small organizations as well.

And finally the organizations that implement best practices or other standards within their organization, such as NIST and ISO, will find the guide even more useful because we include mappings to NIST 800-53 -- also to ISO 27002 and CERT's Resilience Management Model or CERT-RMM.

Julia Allen: I think about, this is great, George, because I think about this jumpstart idea. Because when faced with 19 practices, all these cases, kind of this overwhelming -- because insider threat is obviously just one aspect of security that an organization needs to address, so

Copyright 2013 by Carnegie Mellon University

I think the quick win, a place to start to take an initial step. Have you gotten some good feedback on including that information in the guide?

George Silowash: Since the guide has just been released we haven't received a lot of feedback yet. But I suspect this is going to help a lot of organizations implement an insider threat program within their company or within their business.

I think this will at least help get the practices moving, help the organization get on a path to reducing or mitigating insider threats. We talk about of the some things a small business can do and some things a large business can do.

Generally large organizations have more funding for this type of security measures they might have to implement whereas a small business might not have that same ability. But we try to address that with the quick wins by saying that some of these could be applied to both types of organizations as well.

Julia Allen: Right, because what we've found in a lot of our process improvement experience at the SEI is if you can tackle something that is sometimes referred to as low hanging fruit or something that gives a quick win in a reasonable period of time, that win or that benefit can generate momentum for implementing more of the practices in, for example, in an insider threat program, so I think that's really a nice addition.

So let's talk about -- let's do a little bit, dig into the guide a little bit. As we said earlier, this fourth edition describes nineteen best practices, four new, and fifteen updated that derive from the cases that Lori described. And while we don't have time to cover all of these, we encourage our listeners to take a look at the guide. I would like to spend a little bit of time on the four new practices.

So George, if you would get us started, practice nine, I'll refer to these by number, is called "Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities." So if you could, George, just give us a little brief description of the practice and then maybe talk about a case and a quick win -- that would be great.

George Silowash: Sure, sure. So cloud computing is being used by more and more organizations every day. More companies are implementing it trying to consolidate their systems, save some money. But before a company decides to use a particular cloud service provider, they need to understand and document, assess the provider's physical and logical access and security controls.

The organization needs to be satisfied that the proper controls are in place that will protect the confidentiality, integrity, and availability of data at rest, data in motion, and data in use. It's important for the organization to understand who has access to their data and infrastructure both within their own organization and the cloud providers' organization.

Companies should take these risks into account and should mitigate them to an acceptable level before using the system for production use. In one case, for example, a retail organization used two-factor authentication tokens for remote access. There was a network engineer within this organization who was fired. Before his termination, the insider created a token in the name of a fake employee and a month after the termination the insider contacted the IT department using a fictional name that he had created and convinced them to activate the VPN token.

Copyright 2013 by Carnegie Mellon University

Several months later the insider used the VPN token to access the network and delete virtual machines, even shut down the storage area network, and he deleted email accounts across the organization. It took the IT staff more than 24 hours to restore operations and it cost them more than $200,000 to do so.

Julia Allen: That's a great example. Is there a quick win that you recommend in the guide as a way to get started?

George Silowash: Sure. So one thing with the cloud provider -- you'd need to verify the cloud service provider's hiring practices and ensure that they conduct thorough background security investigations on any personnel.

And when I say any personnel, this includes but is not limited to operations staff, technical staff, and even janitorial staff. We have seen cases where actual janitorial staff has conducted malicious activities within the organization. This needs to be done before they're hired and it should also be done on a periodic basis as well.

Julia Allen: With the cloud service providers though, George, it occurs to me some of these guys are pretty heavy hitters and they're probably not real willing to have their practices be reviewed or have a potential customer do an audit. They can pretty much say, “Take it or leave it.” Do you actually see instances where a cloud service provider is willing to provide the information that you're calling for in your practice?

George Silowash: Sure. Yes, actually there are a couple cloud service providers who actually tailor their services to the regulated sectors like HIPAA (Health Insurance Portability and Accountability Act) or healthcare industry. Also the federal government -- a lot of providers are now starting to customize their services for the federal government because they understand that they have a little bit more rigor and a little bit more controls that they need to have implemented.

So I think organizations need to take a look at the company's operating policies and just have that conversation with the provider to see what information they will reveal. And if that's an acceptable level of risk to them, then they can take that into consideration during their selection process.

Julia Allen: Great I'm glad to hear that. I didn't know about that. It makes sense that the cloud providers would be working hard to meet the requirements of where the controls are more rigorous so thanks for that explanation.

Part 3: Network Behavior; Social Media

Julia Allen: So Lori, let's give you a crack at this. Let's talk about practice 17, which is called "Establish a baseline of normal network device behavior." I worked in intrusion detection and anomaly detection a little bit and this idea of a normal behavior profile is pretty challenging. So could you talk a little bit about that and include a quick win in a case as well?

Lori Flynn: In order to differentiate normal behavior from anomalous behavior on networks, you have to capture and analyze baseline behavior. So every organization has a particular network topology with characteristics such as bandwidth utilization, usage patterns, and protocols that can be monitored for security events and anomaly detection. Deviation from those normal network behaviors can signal possible security incidents including insider threats.

Copyright 2013 by Carnegie Mellon University

So organizations should characterize their normal network behavior at the enterprise, department, group, and individual levels that includes ports, protocols, bandwidth, internal and external connection counts, byte count for email attachment, particular device sets that specific work stations, and servers communicate with, and firewall and IDS alerts. That's just some of what can and should be monitored and analyzed to see what the normals are, what the variation is, and what's unusual.

Julia Allen: So do you find based on your experience, Lori, I mean pardon my ignorance here but I assume there are logging and monitoring and auditing tools that actually help you capture and do the kinds of comparisons that you're speaking of. Is that correct?

Lori Flynn: Exactly. So but often those tools are not put in place so actually this is a good time to mention one of our cases related to this practice. In one case there was an insider who was responsible for research and development projects. And in the four months prior to leaving for a new job, that insider downloaded a high volume of trade secrets including around 17,000 PDFs and 22,000 abstracts. So he downloaded those from the victim organization's server.

Those downloads took place on site and during work hours over just a few 15 to 20 hour periods. So the amount of data that that insider downloaded was actually 15 times greater than that of the next highest user and that data wasn't related to his research. So if there had been monitoring and if there had been a profile of normal behavior, those downloads would have set off alerts.

However the insider's activities went unnoticed until he resigned and it was only after that that the victim organization found out about his downloads. That stolen IP was actually valued at around $400,000,000.

Julia Allen: So what you're saying in that case is that behavior could have been easily detected if the right tools and the right analysis was in place, correct?

Lori Flynn: Exactly. So you had asked for a quick win and I would say that quick win is “use network monitoring tools to monitor the network for a period of time and establish that baseline of normal behaviors and trends.” It's essential.

George Silowash: Yeah, there’s tools out there that will monitor network activity and there is one particular package that I'm aware of that will alert on abnormal behavior. For example, an organization I've seen where they do this was that it would create an alert for anomalous, high activity after hours. So, for example, one workstation for whatever reason is downloading or has network traffic that exceeds a certain limit.

Maybe it exceeds just a few megabytes because you would think after hours there shouldn't really be any activity coming from that computer. So anything that exceeded that low threshold would trigger an alert.

Julia Allen: Right, and it also occurs to me with all the many things that Lori mentioned that could be monitored, perhaps another way to ease into this if you're not doing real aggressive or real sophisticated monitoring is just start with an area like you were describing George -- data downloads or data accesses after hours. Just start with something small and then ease into the larger monitoring activities, right?

George Silowash: Sure, yes, yes. Organizations should keep in mind too that it's not only commercial tools that can do this. There are also open source tools out there that can help. So

Copyright 2013 by Carnegie Mellon University

small businesses or companies that just don't have the budget to do things like this -- they might want to take a look at those open source tools to help them do this and then if they outgrow them, they can maybe look at a commercial solution as well.

Julia Allen: Great. Thank you both for that discussion. So George, let's talk about the third of four we're going to discuss today. This one should be a little fun because it's so much on the forefront of all kinds of reporting.

So practice 18, "Be especially vigilant regarding social media." Something we tend to get pretty hammered with day in and day out but can you say a little bit about that one?

George Silowash: Sure, sure. It seems nowadays more and more people just want to share everything, post everything that they are doing online. Nowadays many people are using social media to keep in touch with their friends, their family, and even their colleagues. So organizations need to be aware of some of the risks that this poses to them.

In particular, an insider using social media can intentionally or unintentionally threaten the organizations' systems and data. Information posted to social media sites could be used to conduct a social engineering campaign against the organization and its employees.

Employees need to be aware of the risks associated with posting information online -- not anything about the organization itself but also their own personal information just to protect themselves. I feel the only way to accomplish this is through proper training.

Training needs to be provided that addresses the policies and procedures about how employees, business partners, and even contractors should use social media. The training could even discuss dangers of inadvertently posting personal information online that may cause financial or other loss to the employee.

Julia Allen: Great, so how about a case?

George Silowash: Sure. So an attacker compromised the email account of a former U.S. vice presidential candidate. The attacker simply used a search engine to find the answers to password recovery questions which included the date of birth, the zip code, and where she met her spouse.

All these answers were found online through simple web searches. The attacker used this information to reset the password on the account and he proceeded to read through her email and posted it to a public forum.

Julia Allen: Well, that is probably something that could happen to all of us. Obviously someone in that role pulled a pretty high profile but any of us could be subject to that kind of an attack, correct?

George Silowash: Sure, sure. I mean just even looking at, for example, a Facebook profile that somebody -- a lot of people post a lot of information about their personal lives on there. How much of that information could be used to reset somebody's password on any account? I mean there's a lot of information could be gleaned just by looking at that person's profile page or just doing some other simple web searches.

Julia Allen: Right, and how about the quick win?

Copyright 2013 by Carnegie Mellon University

George Silowash: Sure. So a quick win for this one would be for the organization to include social media training as part of the organization's annual security awareness training program.

Part 4: Data Exfiltration

Julia Allen: Great. Well, Lori, you have the honor of discussing with us the last practice, practice 19 "Close the doors to unauthorized data exfiltration," which just by title seems to perhaps relate it a little bit to the one you previously discussed although for network device behavior the employee was inside. It seems that one of the things you want to watch for is stuff going outside, right?

Lori Flynn: Yes, yes. And data exfiltration -- well first of all I'll define what it means. It means the organization's data moves to an unauthorized place. So that can happen electronically or through physical means such as printing out documents and just walking out with them or carrying a thumb drive with data, the organization's data on it.

So to address data exfiltration in general, an organization has to first of all identify its critical assets. That's information, technology, and facilities. And then it has to identify people who should have authorized access to those assets as well as those who actually do. And lastly, it has to determine the asset locations, the physical asset locations, for all of those items.

An organization has to be able to account for all of those devices or all devices, not only ones they own but all devices that connect either physically or wirelessly to its information system. So some example devices that could be used to exfiltrate data includes smartphones, thumb drives, printers, scanners, fax machines, mp3 players, microphones, and even video conferencing systems.

Internet services like instant messaging and SSH, FTP, and email can be used for exfiltration as well. Smartphones, in particular, can exfiltrate using private connections, private internet connections, that the organizations cannot monitor. So these are just a handful of example ways that exfiltration can be done and the organization really has to look into all possibilities to try to protect against them.

In order to protect against exfiltration, a combination of strategies need to be used together: policies, technical controls, compliance checks, and physical controls can all help to prevent and detect data exfiltration. The challenge is really to balance security with productivity. The controls need to allow authorized information exchanges but also prevent unauthorized exfiltration as much as possible.

Julia Allen: Right, because as I'm thinking listening to you describe this practice, this can be pretty daunting particularly as we talk about BYOD, Bring Your Own Device, and all these, as you mentioned, this proliferation of both organizational and personal devices that are connecting to the network -- very, very difficult to get your hands around.

So I think one of the key things you said is to identify the critical assets because it seems to me, would you agree, that you can't necessarily inventory and monitor all of these but you want to pick the ones that are most likely to be involved in or most at risk if data is exfiltrated either onto them or from them, would you agree?

Lori Flynn: You can pick the most at risk items. Additionally there can be general policies. An organization has to determine if a policy, say for instance, against bring your own device, if the security it would provide, the added security it would provide if the cost in terms of employees being maybe dissatisfied if they didn't have their smartphones in their pockets. That cost has to be weighed as well. So organizations first of all have to determine what the risks are and then make a decision about return on investment.

George Silowash: So this practice could be a little bit tricky for organizations to implement. As I like to say, "You need to know what you must protect." And a lot of organizations can struggle with this one because their data is just scattered everywhere across the organization. It can be on servers, workstations, people's personal thumb drives. It can be on their local machine just sitting in their local documents folder and they need to get their hands around where all that data is at and understand what type of sensitivity it is. I mean, is it something that a company considers confidential, proprietary?

They need to put proper security protections around that information. Actually we have a couple of tech notes that are being released; two which have already been released. There's two more in the queue that actually talk about data exfiltration and understanding where your data lives.

One of them actually addresses an open source scanning tool that will actually go out there and scan your network looking for sensitive data. So in order to implement this one I think one of the biggest challenges is knowing where your data lives and how to protect it.

Julia Allen: That's good advice. So how about a case?

Lori Flynn: Let's see. In one case, a tax preparation service employee, an insider as a tax preparer and while that consultant was on site and during work hours, the insider printed personally identifiable information on at least 30 customers and then the insider later used the Social Security number information to submit fraudulent tax returns using those IDs. The refunds totaled $290,000.

Julia Allen: Okay, and how about a quick win?

Lori Flynn: Restrict data transfer protocols, such as FTP or SCP, to employees with a justifiable business need and carefully monitor their use. Those kind of protocols can export a lot of data quickly so that's a good, high impact win.

Julia Allen: Excellent. Thank you for all those examples. I really appreciate it. So we're coming to our close. This has been a very rich and information-filled conversation, which I appreciate and hopefully have encouraged folks to look more into this subject. So with that in mind, George, do you have some resources where our listeners can learn more?

George Silowash: Sure. The fourth edition of the Common Sense Guide is available on our website. I encourage everyone listening to review and share the document across the organization and discover how it can help the organization better prepare and defend against malicious insider attacks.

CERT's Insider Threat website has a wealth of additional information including technical controls, some technical notes that can be implemented to mitigate insider risks. The site also has links to our previous podcasts and our insider threat blog.

Julia Allen: Great. Well first of all I'd like to thank you both so very much for your time, for your preparation, for your expertise. This has been a great conversation. So first of all George, thank you for participating with us today.

George Silowash: Sure, great thank you. I really enjoyed this.

Julia Allen: And Lori, any last thoughts? I would also like to thank you. Is there anything else that we haven't covered that you'd like to add?

Lori Flynn: Thanks so much for having us. Let's see. I guess just like George I would direct people to our website. We've got a ton of information that can help people to prevent, detect, and respond to insider threats.

Julia Allen: Great, well thank you both so much.

Copyright 2013 by Carnegie Mellon University