Integrating Security Incident Response and e-Discovery
Transcript

Part 1: Information Security for City Governments; Defining e-Discovery

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 web site.

My name is Julia Allen. I'm a senior researcher at CERT working on security governance and software assurance. Today I'm pleased to welcome David Matthews, Deputy Chief Information Security Officer for the City of Seattle, Washington. Today David and I will be discussing an approach for integrating computer security incident response with e-discovery, where electronic information is requested as evidence in legal proceedings. So, David, so glad to have you with us today. Thanks for being here.

David Matthews: Glad to be here.

Julia Allen: So before we get into the e-discovery part of our conversation, kind of just for general interest, what are some of the unique aspects that you've found, or differences, in managing information security for a city versus either a commercial or business concern?

David Matthews: My experience is that generally we have less resources for one thing. We have a staff of two and any budget we get we basically get by schmoozing with the other divisions around here, operations mostly. So we don't have a direct budget of our own. So that's one difference, of course, one challenge.

And then the other, I think, is probably the biggest challenge, or the biggest difference is the difference in the executive buyoff, which I think everyone who works in information security recognizes as one of the most important things when you're trying to do information security. And it's a little difficult when the executive is elected every four years and their priorities are really more around visible things like potholes and supporting the arts or the police, things like that. And generally the executive level just has less of an understanding of what information security risks are. So we have an education process that we go though here.

The other thing, I guess, we're a federated group. I think this is true of a lot of organizations, or government organizations, especially municipalities and counties and that kind of thing. It's kind of a federated group of several different, 50 actually, 50 or more in the City of Seattle, different lines of business. So that includes the utilities, public safety, justice, legislative department which is the city council, the executive, of course, the mayor's office and everything that attaches to that, transportation and all the rest. All of those tend to operate in their own silo. We've done a lot of work here, and I've actually made a lot of progress in standardizing IT governance and operations, but the old ways are kind of hard to break through.

And so information security being a relatively new thing in the city, is still having some challenges in getting people to work together and really be on — do information security risk management and all of this on a city-wide basis instead of just in their own silos. But we are making good progress, but I think that's some of the differences in working in a city government, anyway.

Julia Allen: It seems to me with the breadth of services that a city government has to provide, and as you said you've got elected officials so you don't have the kind of duration for your senior leadership. And clearly their attention is going to be directed toward things that are related to the citizenry. And so you usually don't hear a big hew and cry out from the general public for more information security, at least on a broad base, certainly in selected areas. So I can imagine that some of the challenges are fairly unique when compared to your colleagues in for-profit concerns.

David Matthews: I think the one thing that does get the public's interest is privacy issues, so we leverage that to some extent and we try to bring that to the executive as the ROI for us. Return on investment for us is ensuring the public that their data is safe with us. That's still, like I said, it's kind of an uphill battle and it doesn't — and it seems to be hard to get that message. But that's the one we work with the most and seem to get the most traction out of.

Julia Allen: Well to kind of turn our attention to today's topic, what is e-discovery, kind of how do you use the term and how do you see it showing up?

David Matthews: Sure. Well, just a quick definition, I think of e-discovery in the first place, is it's basically in any legal process there's what they call the discovery phrase. The two opposing parties get together and discover. They agree to discover and disclose any relevant evidence that regards the case. So electronic discovery or e-discovery is simply the discovery and disclosure of that electronic information, what they call ESI or Electronically Stored Information that everybody holds.

The reason that e-discovery had become so important recently is it's really come to the forefront and people have recognized that electronic evidence, electronic data lives everywhere. It's ubiquitous. It's in our phones. It's in our cars. There's just electronic data everywhere and we all create records everyday as we walk around, and many of those are created electronically. So this is where e-discovery really has become important recently.

Julia Allen: And I would also think with kind of the proliferation, as you said, electronic information is everywhere. The notion of knowing exactly what kind of information to pull or kind of, on the other side, that you could actually be buried in e-discovery requests, tends to make the electronic aspect of information in a legal proceeding very challenging.

David Matthews: In many cases, and I know this is the case for the City of Seattle, it's quite often the case that they just settle rather than get buried by these e-discovery requests. So it's become a weapon in the hands of the plaintiffs' attorneys to say, "Well, we'd like to see everything that you ever wrote, every email that was ever created in regard to this case." And it's so much money and time involved to do that it's easier to just settle out of court. So a lot of cases don't even get to court just because it's the way e-discovery has gone and the proliferation of electronic evidence.

Part 2: Being Prepared for an e-Discovery Request

Julia Allen: So what are some of the actions or practices that you've seen be effective, that security professionals need to take under consideration or implement so that they're prepared when an e-discovery request shows up at their door step?

David Matthews: Well, there's some basic information security risk management practices that I think most of us do anyway, but that you kind of have to take it a little bit further. One of those is understanding where your data lives. Understanding very specifically who owns the data in your organization, who has access to it, where it's stored, what devices or media it might be on, and that's a pretty big list sometimes. And things that people don't think about sometimes are like the access, the door access key card information or the video — now that a lot of video files are digital first — the video cameras, the security cameras, iPods, and game consoles.

There's all these new devices that people can put information onto, and to recognize that and understand that and really have a good understanding in your organization, where are all the places that data could live? And how would you access it if you needed to access if for e-discovery? How long would it take? How much would it cost? And then if you do have to get it, what do you have in place to preserve it forensically and carefully so that you can actually prove the integrity of it if you need to in court?

That's kind of a first step, but then I think the next step is to go meet with your counsel — outside, inside whichever one you're working with — and discuss that. Make sure they understand this information because they need to know when they go into court, or when they get a filing, they need to have an understanding of where they stand in order to — as far as the electronic evidence, as far the electronic data is concerned.

Records management is another group of people you need to become familiar with. They're the folks, if you have a specific records management organization or a division as part of your organization, they're the folks who know what the rules are around when records are supposed to be kept and how long, and whether they're supposed to be deleted. That all is germane when you get into court. You have to be able to show that you followed your records management procedures carefully and that you've monitored that. So you need to meet those folks. And you can spend some time with your law department, your legal counsel developing a litigation hold process and litigation hold policies, and developing data preservation and analysis procedures. You've got to have your executives understanding how important this is and law can really be helpful in this, I found.

I've sat down with our lawyers and talked to them about this, and once they were onboard with this, the executive tends to listen to the lawyers. At least that's been my experience. They have a lot of respect for them and often the lawyers are involved with their public information and that kind of thing, and public disclosure requests etc. So they tend to listen to the lawyers, and so the lawyers can be a great ally when you go to the executive and make sure they understand what the risks are and how important this is.

We talked about records management policies and litigation hold polices and all these procedures that are important to get into place, but none of that is any good if you haven't trained the users on all these things. If the users don't understand the policies and procedures, and if you don't have some way to show audit and show that they've actually learned these procedures and policies, that they follow them regularly and that this is in the regular line of business you do this stuff on it. And that gives you something to stand on if you have to go to court and show that, "Yeah, well you lost some data, but it was in your normal line of business. You deleted that because that's the records management policy, or the litigation hold was in place and everybody knew about it, and so we did everything in our power to make sure the data was there." So that's kind of a quick step through some of the things I think are most important.

Julia Allen: Well, it's really fascinating for me being a security researcher and professional that we tend not to think about this whole area of, as you say, records management, information management, forensics investigation, e-discovery — the whole legal side of how this information can be used. And so it just seems kind of like yet another whole new area of competency and skill and attention that we need to pay when we've also got all kind of the standard security and risk management things to do.

David Matthews: Yeah, it is. It has — for us it's become a whole other job that we have to handle. I've talked to the lawyers quite a bit here at the city about creating a whole new division that does nothing but this — nothing but the litigation process, nothing but the e-discovery process. It could be easily tied in with the forensics practice that we have. It all kind of ends up being tied together anyway.

A lot of the forensics that we do, I do mostly, has to do with policy violations, and often those lead to employment issues, and those often lead to law suits. So it all fits together anyway and it's all kind of the same practice. So they do all meld together in a way.

Part 3: A Common Process: Incident Management and e-Discovery; Key Roles

Julia Allen: Well, I think one of the shining lights, or one of the light bulb moments that I had when you and I last spoke that might help get some traction on this, is you had told me that your office is making progress in doing some integration between all these growing number of e-discovery requests with your security incident response processes, which are probably a little bit more mature, and I'm kind of curious as to why you headed down this path.

David Matthews: It really just made sense when we started comparing the way these things work. We created our incident response plan using the government's ICS NIMS which stands for National Incident Management System and then ICS is Incident Command System. So those two together — they were actually originally built, created by forest fire, wildfire fighters and it's been created and built up as a system for incident management, a standard system for incident management that any government organization will use. Mostly first responders, firefighters and police, are familiar with it but we've taken it on as a good model for any kind of incident response. And the good thing about that is that then we scale up if we need to scale to another organization or if we need to scale out to a larger group, we're all speaking the same language. But anyway, that's how we developed it.

The event management process, the basic steps in that process for us, is kind of first of all is just kind of recognizing what the problem is, so triage. And then gathering our subject matter experts and stakeholders together and finding out more about what's going on in the investigation part of it, creating a plan of action, going through the plan, etc. And then all the kind of rinse and repeat; evaluate what happened and then go back and investigate some more etc. And then of course the lessons learned part at the end.

But when we started looking at our incident management process and comparing that to how our e-discovery procedures go, it really is the same thing. There's probably a different group of subject matter experts in the room possibly. They've just got to include some lawyers. And the action plan includes this litigation hold process. But really if you start comparing one to the other it's very similar and so it just made a lot of sense to go that direction.

Julia Allen: That does kind of make sense because you think about an incident can be anything, as you said. Some of the processes that you've adopted come from firefighting and probably other types of emergency response. But it's just that the idea that e-discovery which tends to have kind of more of a legal connotation where as security incident response seems to have more of a traditional information security, and maybe even more of a technology focus — you tend not to put those two together. And I think that recognizing the commonality, particularly when you're in an arena where you're resource constrained, as you find yourself and we all do, it can be very beneficial.

David Matthews: Sure.

Julia Allen: Have you found good uptake in the organization and with the people that you work with? I mean, is the view of the common practices and steps in the process fairly — have people been fairly receptive and seen the connections as well?

David Matthews: Definitely. We've made some really good progress with it. The attorneys were very thankful when we finally sat down with them and started walking through the process and trying to put some pieces in place and some procedures in place, some documentation and that kind of thing. So now they call on us basically every time there's a litigation. They call us up and have us do the scoping meeting with them and decide where the data lives, how we're going to get it, who's going to get it and that kind of thing. So it has worked out pretty well in that regard. And really the acceptance amongst not only the attorneys, but amongst the IT folks has been really well, really great, because they are very happy to have some guidance. Up until now it's been pretty ad hoc. Everybody just kind of felt their way along and nobody quite knew what was going on. So to have somebody come in and say "Here's what we're going to do, and here's how we're going to do it, and here's the steps we're going to take." I think everybody from the IT folks who have to do the acquisition to the attorneys, of course, but also the users or the management or whoever else has that relevant data, they're all very happy to have somebody guide them and give them the steps that they have to make to make sure that's it's done well.

Part 4: Key Roles; Steps for Getting Started

Julia Allen: So do you have a standing team that is kind of prepped when either a security incident needs to be investigated or an e-discovery request comes in? Do you have kind of like just a standing group or a permanent group? Or do you tend to bring the parties together so you've kind of decided in advance who needs to be involved in what types of events and then you bring them together when the event actually occurs?

David Matthews: Well we don't really have a standing team. We have this federation of organizations here, so depending on which organization is affected we have — we gather the subject matter experts from that organization. Now, there is a citywide messaging team that handles email for most of the city, although there's a couple of utilities who have their own email folks as well. And the police are separate because they're the police and they do everything separate. So, again, but I still work as kind of the coordinator for any kind of forensics or investigatory incident including litigation hold. I could walk you through an event? Would that be a good example?

Julia Allen: Oh sure, yeah, go ahead. Kind of summarize for us what happens.

David Matthews: Sure. So imagine, just imagine a certain local government had a disagreement with a local sports franchise, for instance. Just imagine such a thing. So I'm asked to assist with the e-discovery thing. The attorneys call me up. So then you can compare it to any other event.

The first thing they do is triage. What's the most important, the highest priority and the most likely place, basically, to find this data? We want to know who's going to have the email. That's probably the biggest thing. Almost always it's the email. So we go first of all to the email staff, or to the staff of the organization that was handling the contract, say. And we get them together and we say, "Okay, have you preserved this email already? If not, what do we need to do to preserve the email?" We get a hold of the email administrators right away and we tell them to stop any purging that's going on of the user's email that might be relevant.

And then, again, as with any cyber event, you gather the subject matter experts. So we want to get the IT people who manage the servers together. We want to get the management for any users who have relevant data. We want to get those users in the room, and of course the attorneys. And we want to all sit down and really make sure we understand the scope of the issue. Where's the data? Who owns the data? Who's going to be responsible for gathering it? How are we going to preserve it? How are we going to do it in a forensically sound manner? Who's capable of doing that? And then evaluate, make a plan to do that. So it really kind of follows the same steps as any cyber event. We've got to go through that process and then go back and make sure it's covered.

I think probably one of the important things to note here is that what I said about acquiring things in a forensically sound manner isn't something to take lightly. The people who do that acquisition have to have been trained to do it right, or someone has to monitor their every step, and you have to document that. Because that can come up in court and be a bone of contention, or something that could really hurt your case if the court can show that you didn't take care of the evidence carefully enough. You didn't maintain the integrity and you didn't maintain a chain of custody, so that anything that they could attack to say "This is not really the relevant evidence or you didn't give us all the relevant evidence." So I think that's a very important note about that.

But anyway, that's sort of a step through of how we would do it and then go back again after the fact. There's a litigation hold form that we issue. We go back after the fact and say, "Have you preserved all this data? If so sign here," and we have that as documentation that they did do their best to find all the data. And then we go back and ensure that they've done that and follow up with the folks who have relevant data to make sure they're continuing to hold onto data as long as the case — as long as any relevant information's being generated.

So it can be a long process. Cases can go on for years. Sometimes people have to be on litigation hold for several years in a row and that can be a challenge as well as just for the basic matter of storing and preserving data in a way that you can prove the integrity.

Julia Allen: Well, if a business leader or an organization kind of wanted to start down this path — I suspect many of them are dealing with it already — but if they wanted to really take a hard look at integrating their e-discovery and incident response processes, what would you recommend as some of the first steps to take?

David Matthews: Well, I think the very first thing is to make an appointment with your lawyers. Get the attorneys and the IT staff, the information security — information security is a great group to have in the room with you. Somebody at that conference we were at said that he actually, as an investigator or as an expert witness, will often challenge the evidence of the other side based on whether or not they have a good information security program. And that's simply because the information security program is all about the integrity and preservation of data.

And so really they need to be there in the room. They can be a great ally. And so as management, as management and leaders, get your information security folks in the room. Get your IT management together with your lawyers and your risk mangers and your records managers. Get them all in the same room together and start talking about all the things we've talked about here in this podcast. Think about where the data is and who's going to control it, or who has control of it and how you're going to get to it if you need it. And then do you have an incident response plan in the first place? Start with that. And if so then see how that can be integrated into a litigation hold process. They all kind of fit together.

You assign that task to somebody who will bulldog it through, basically, and make sure they have the staffing and resources to do it. But if you give somebody that responsibility and you know you can trust them to do it, you should be able to put together a program similar to what we have and what some of the more mature organizations out there are doing that I think will serve you very well in the event of litigation, which is basically, for us, a daily event almost.

Julia Allen: Well, David, I feel like we've probably just touched the tip of the iceberg. But do you have some good sources that you can point our listeners to for more information?

David Matthews: Sure. Just to start I really recommend, as far as putting together an incident management process, the FEMA (U.S. Federal Emergency Management Agency) training site. The NIST (U.S. National Institute of Standards and Technology) also has some really good incident response information and checklists that you can go down through. And then as far as the e-discovery stuff, there are a lot of good sites out there. And I think I'll go ahead and send you a list of links that you can post on the site that people can go to.

Julia Allen: Okay, well we'll certainly include all of that information in the show notes.

David Matthews: Sure, and I'm always happy to share as well.

Julia Allen: Well, David, I really do appreciate your time and your sharing your expertise with our listeners today. I've really enjoyed talking with you.

David Matthews: It's been a real pleasure. Thanks for inviting me.