The Real Secrets of Incident Management
Transcript

Part 1: Communication Is Key

Stephanie Losi: 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 Stephanie Losi. I am a journalist and graduate student at Carnegie Mellon, working with the CERT Program. I am pleased to introduce Georgia Killcrece and Robin Ruefle, who are members of the technical staff at CERT, and they have worked extensively to help organizations develop incident management capabilities. Today we'll be discussing incident management lessons learned, as well as tips for building and sustaining an incident management capability. So, Georgia and Robin, welcome.

Georgia Killcrece: Thank you.

Robin Ruefle: Thanks.

Stephanie Losi: Why should leaders care about incident management?

Georgia Killcrece: Well, before we answer that question, it's nice to just step back and look at it from a broader perspective and say: even in the face of protection strategies that you put in place to protect your business assets, your information assets, there are still problems that can occur, so even the best defended network can still suffer attacks, and there will still be risks. And so when incidents do occur, one of the goals of having an effective incident management capability in place is to ensure that you quickly identify those problems, that you're quickly able to respond to those or mitigate the effects of such attacks, and then get the business back on track to do its day-to-day operational work, and so you don't lose any functionality. And so the speed that an organization can bring to bear to answer and address those concerns can lead to its success overall.

Stephanie Losi: And so how would you define an incident?

Georgia Killcrece: Well, for us an incident is, let me step back and say we characterize events as sort of anomalous activity -- any kind of an activity that occurs on a system, whether that be a probe or a misuse of an account or whatever – and those events then by virtue of some criteria that an organization has identified can move into this area called an incident. So it's identified as an incident, an attack against a system that meets those thresholds.

Stephanie Losi: Right, because maybe it's malicious, maybe it's not.

Robin Ruefle: There's a lot of different types of events also. So when you're looking at events you're not just looking at technology. It might be something that's organizationally or socially related that's going to cause some kind of [activity], whether it's criminal activity or some other malicious behavior, and then how do you synthesize that all down and determine what is really a computer security incident for your organization — and different sectors may have different definitions. But the thing you want to do is make sure that everyone in the organization understands that criteria.

Stephanie Losi: What would you say is the most critical issue that you see currently facing business leaders who want to build a capability for incident management? And also, like what's their most important determinant of success, what are some lessons you've learned over time, and what are some common problems that can crop up?

Georgia Killcrece: It's hard to come up with one answer to that. At the very front of the pack is the lack of an enterprise view into incident management activities, because traditionally it's all been about, "React. React to a problem," and one of the lessons that we teach in our training courses and in interacting with customers is that in order to win this game, you have to get ahead of the curve, you have to get to the point where you're being more and more proactive, and so lots of organizations are looking to try to do that.

So for our purposes, when you look at incident management, then you're saying, "Well, it's not just a group of people in the IT department who are reacting to whatever today's events or incidents are." It's looking at the whole end-to-end activity that might include more than — and most assuredly does include more than — just that component that is in telecommunications or the IT area. So you're looking across the organization, and that pulls in people like your business owners and operators, your human resources, your public relations or media folks. It could involve law enforcement, it may involve the legal department. So it really is spanning a much broader area, and if you want an effective incident management capability that looks beyond just reacting, then you do need to pull in some of those other parts of the organization to talk about those activities.

Stephanie Losi: And so how do you set up sort of a working communication process? You know, who makes up the core team and who makes up extended members of the team, and how do you manage communications between the core team and the extended members in such a way that the extended members, you know, they can do their jobs but they can also participate in incident management as needed?

Robin Ruefle: Well, one of the things to look at too is — and people in our courses and when we talk to them don't always like this answer, but — it's not always the same for each organization, and so there's not one right way to do something. When you look at a set of best practices and you look at some common problems to avoid, or you look at some common success factors that you want to build in — I mean, that will help you move along the path, but it's not just one set of things that you might do.

Georgia Killcrece: One of the problems that we see is that often times the key players are not involved in the loop, and so you have the right hand not knowing what the left hand is doing, and that can be a problem if there is something that involves a security event.

Let's use, for example, maybe there's personally identified information that is exposed, and if only one part of the organization deals with and handles that activity, then what happens at perhaps a higher level management where they don't know about that? And we've seen some of those already appearing in the media, and some of the aftereffects of those kinds of attacks, and that's just one area that gives an illustration.

There are, you know, many, many more areas and ways in which not having the real clearly defined roles and responsibilities across a team, across those people who are involved in the incident management, can then get in the way of you having an effective response and an effective strategy for continuing the operation or the mission of the organization.

Robin Ruefle: And, in a way, what you're bringing up and asking about that communication, that's one of the key areas, just as Georgia was saying, is it's really you having that information and making sure all the people have that information too. So it starts even with the end user, whoever's using the computer services, do they understand what is a malicious activity? Or what do you want them to report back to you? Do you have a form? Do you have any guidance that you can give them? Where do they call? Do they call a help desk, do they call a CSIRT number, do they call some other number? How does that information get passed on to the actual technical analysts? Who are those technical analysts that can actually determine, "Is this a computer security incident, do we know about it, what can we do to contain it, to fix the problem, and to ensure that our organization continues to function?"

So, looking at that different type of communication that goes on, and as Georgia was saying, when you think about all the different people who might be involved, when we go in and we actually work with organizations to set up an incident management capability, or we go in and we evaluate organizations to see how well they're doing, one of the things you want to look and see is, what is the actual path — to lay out that path, see who's involved, and then get the right people talking together, like Georgia was saying.

Georgia Killcrece: Right, and if you take it up a level and look at it from what's happening out in the environment, one of the other drivers is what kind of regulations, whether they're federal regulations or laws in a different country that apply to organizations in that country. There may be requirements that say they have to do certain things as it relates to cyber threats and reporting incidents. And so those, too, come into play as organizations are deciding what do they need to have in place to effectively deal with cyber threats and cyber incidents.

Stephanie Losi: Right, you were mentioning the personally identifiable information, and I know a lot of states recently passed laws saying, you know, if a resident's personally identifiable information is revealed you have to report it, but the executive can't report it if they don't know.

Georgia Killcrece: Know about it, right, right, and if, as Robin said, the end user doesn't know what to do in those cases for reporting it, then you can have breakdowns and failures all the way across the organization with people not doing the right thing with the information.

Stephanie Losi: Right, and I mean the end user, you know, may be afraid, may feel like, "If I report this, you know, I'm going to lose my job," or it may never have been even really, you know, articulated what will happen.

Georgia Killcrece: Right.

Robin Ruefle: And this is also something that ties in with that whole communication [issue], because what a common problem that we've also seen is that that information may get reported, but reported to some different area. And it never goes back — to when we look at incident management capability, you want to look at all that information and all the different types of incidents coming together so you have a repository of information, so you can correlate data and see, "Have you seen this before, do we know what the remediation strategy is?" anything like that. And if the information is not getting to the right place, then you could be missing a lot that could damage your organization.

So when you think about the fact that you want people to all understand it, so that if it gets reported in some small help desk out in the field, it gets to the right people who can handle the computer security incident, so they need to understand it and know how to pass it on and to who to pass it on.

Georgia Killcrece: Right, and so thinking in terms of incident management or just CSIRTs in general, what they're looking to do is get that bigger picture of what's happening across the organization, whereas the help desk may have a very limited view of what's going on, [or] the IT department has a limited view of what's going on – they're responsible for the infrastructure, they're responsible for making sure systems are configured correctly, that patches are rolled out, that AV software signatures are up to date, but they may not be looking at what other parts of the business functions may play into this broader, larger incident management capability.

Robin Ruefle: And even who the point of contacts are, so if you've determined something is criminal in nature and needs to be reported to law enforcement, well, what's the process? Who is actually that point of contact to call law enforcement? Where does management get involved? In some of the courses that we teach, we talk about the whole area of response. It's not just technical response. There's like management and administrative response, dealing with business actions that executive managers may take, new changes in policies that they may instill. There's human resources that may get involved if it's an insider and you need to remove an employee in a fashion [so] that your systems aren't damaged. There could be public relations [involvement] if information has leaked out about something bad that's happened to your organization.

So there's a lot of different areas that need to be involved from the management-administrative side, and then there's the legal coming in. Are there any liabilities? Are your service level agreements for your main function of your organization going to be affected? So there's a lot to think about, in that communication, collaboration, coordination.

Part 2: Data Flow in the Real World

Stephanie Losi: Great, so what can an organization do to make sure all the data is flowing into the right place? Are there particular steps that someone can take, or just a plan that they can put in place?

Georgia Killcrece: Well, I think a plan, as we talked about earlier, of having effective strategies in place and communicating what those strategies are to the rest of the organization is critical. Certainly, from our past history, we have seen that this is a relatively new profession, new field of work, and so traditional incident response/incident handling tools are being developed, and they still continue to be improved, but you can't go out to your local Best Buy or Circuit City and pull off the shelf the, you know, end-all security tool for tracking incidents in a robust tracking system. Many tools are emerging, but they are still in their infancy and they still do need to have some improvements to them, but we're seeing that happen.

So, having a way that you can quickly identify information; a searching capability; an ability to be able to collect information that may be adjunct to the actual report, so log files that could be associated with an incident report, maybe some directories, some analysis results that can be attached to that or somehow accessible through the tracking system; having a capability to have incidents in various states of investigation and be able to sort and queue up and have reminders for those kinds of tracking activities. And also because this is a global Internet society that we are involved with, incidents happen everywhere, and they can come from everywhere. And so the need and the mechanisms to be able to share information in sanitized ways with your external partners, with external teams that may help you in contacting or running down where an attack is coming from, being able to communicate and track those incidents through some common mechanism for reporting, collecting data, sharing data, communicating data, all of that comes into play.

Robin Ruefle: And it all ties back, too, to thinking about this as an enterprise view. When we think about computer security incident response, we always say response doesn't happen in isolation, and any type of incident management capability or incident response team, whatever you want to call that, has to be supportive of the main business mission of your organization. Now there's where some conflicts can sometimes come up, because you may have the technology to prevent an incident or to contain it, but that may cause you more business function problems by taking out your main services.

Or there may be cases where we've seen, for example, there are systems in the health area that have certain FDA certifications, and they can't be patched without breaking that certification. So how do you get around that? So everything has to be thought of at that enterprise view. You have to think about the fact of, what is the main business function of our organization, and how does the incident management capability support that by keeping those systems protected and up and running? And tying into that information repository that Georgia was talking about, one of the things that's critical to have is an idea of, what are your mission critical assets, systems and data, and where are they?

And so you can see again that there are ties into other parts of the organization. The people who are actually handling the incidents — they're not going to have the risk management skills and expertise, but they need to be working with people who do have those skills. So if someone calls in to the help desk and says, "Such and such a service is under attack," do you know immediately, to help you assess the threat, how critical this is, can I even patch it, can I take it down, can I do any type of mitigation, what kind of problems this is going to cause my business?

Georgia Killcrece: And maybe even, who is the business owner of that system?

Robin Ruefle: Exactly. Who do I need to notify? And sometimes it's that business owner, many times, who's going to make the determination of what you can and cannot do. So again, that incident management capability is going to include that coordination with those business managers.

Georgia Killcrece: One of the things that we recently published on the CSIRT webpages is a high-level action list that talks about many of the things that we're talking about today but what's interesting is that serendipitously, this one also brings out some of the common problems. So when you talk about, "What are some of the pitfalls to avoid?" in that document we kind of list very high-level, it's certainly not a comprehensive document, but it's just a quick list, a quick action list, if you will, of steps that people can take to build that kind of a CSIRT or an incident management capability, and then some of the typical problems that we see when we're out there in the field talking with other customers, talking with other incident response teams — problems that can cause some failures.

Stephanie Losi: This is available on the CERT website?

Georgia Killcrece: Yes.

Part 3: The Future

Stephanie Losi: Great, so let's close by talking about how we might see incident management evolving over the next few years, and what can business leaders do right now to be prepared for that when it does happen?

Georgia Killcrece: We are seeing more push in the community for having ways to evaluate capabilities, and so we are beginning to see the emergence of standards, like the ISO standards, the ITIL standards, the NIST Best Practices, some of the Federal Information Processing Standards, as well as certification – certification not only of teams but certification of individuals who are performing the work on behalf of those teams within those organizations. We see all of that coming down the pipe, if you will.

Robin Ruefle: And really, if you think about it, as far as a discipline, incident management as computer security incident response, is still fairly young, and so we're really moving into that phase. We're looking to standardize and, as Georgia was saying, and looking at really developing those best practices, seeing if there are things that are common to particular sectors or not. We often get the questions, "Well, where does incident management fit in disaster recovery, or continuity of operations, security incident management?" and the thing is that they're not all separate. They have overlapping pieces.

And so you have to think strategically at a high level about, really, how does all this fit in your organization? What are the triggers from incident management, the information that you may get as you're responding to an incident, that is going to trigger the people who are handling the continuity of operations, or a disaster recovery if it's even more severe? So really looking at how does this all fit together, and thinking about what type of plan and response do you want in place that's going to be able to be a repeatable process, that's going to be quality [driven], that's going to minimize the damage to your organization, and keep things running, keep that meeting the mission of that parent organization.

Georgia Killcrece: We see in the community that organizations put in place business resumption, business continuity, contingency plans, backup plans, and so one of the things that we often see in organizations who are beginning to build capabilities such as incident management capabilities is that they're very thin, they have one person deep and they're stretched over, and they may wear multiple hats. And so just as the organization is building these, you know, contingency plans and disaster recovery, we also need to think about terms of not having single points of failure in an organization. So if you have one person who is this, you know, wonderful, technologically savvy person who is handling every aspect of your incident management response activities or CSIRT activities, and they leave and go work somewhere else, then all of a sudden the house of cards falls down around them.

Stephanie Losi: Right, or what if something really goes wrong, and it's more than that one person can handle?

Georgia Killcrece: Can handle, right. So we need to think of those kinds of approaches as well when you're looking at the incident management functions or building a CSIRT capability.

Stephanie Losi: Okay, well thank you very much, Georgia and Robin, this has been great. I appreciate your time.

Georgia Killcrece: Thank you.

Robin Ruefle: Thank you very much for having us, Stephanie. We enjoyed being here.