Computer Forensics for Business Leaders: Building Robust Policies and Processes Transcript

Part 1: Why Policy Is Key

Stephanie Losi: 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 Stephanie Losi. I am a journalist and Carnegie Mellon graduate, working with the CERT Program. Today I am pleased to introduce Cal Waits, co-author of the First Responders Guide to Computer Forensics and a member of the technical staff at CERT. We'll be building on a previous podcast, A Computer Forensics Primer for Business Leaders. Our discussion today will focus on the specifics and challenges of establishing robust, repeatable processes for incident investigation and computer forensics. So, Cal, welcome.

Cal Waits: Thank you.

Stephanie Losi: One challenge facing business leaders is that they need to understand how to support their first responders, who are often system administrators. So what would you say are some must-dos for business leaders who want to give first responders the level of support they need to successfully investigate incidents?

Cal Waits: I think preparation is the key. You want decisions made primarily before 3 a.m. on a Saturday morning.

Stephanie Losi: When there's a disaster, right.

Cal Waits: In the middle of a disaster, you don't want to be trying to figure things out then. So things need to be discussed, they need to be decided. Obviously, you can't consider every eventuality, but having guidelines in place and an understanding on how problems should be resolved goes a long way towards clearing those things up.

Stephanie Losi: All right.

Cal Waits: I think understanding the need for policy, as well as driving the creation of the policy, is the key role of the business leader.

Stephanie Losi: Great.

Cal Waits: They need to sort of champion that aspect of it. The actual, the specifics in the policy, that should be left obviously to people that have a more detailed understanding of the technologies involved. People from various departments that have different responsibilities and different strengths will help, but driving the creation of that policy is where the business leader comes in.

They're in a position of power to move things forward. And if it's left just to chance or sort of an ad hoc affair, you can end up with a really muddled response to any sort of incident. And that kind of a response, a muddled response, can result in either a) not actually finding anything out, or b) the things that are found out can't be used in any meaningful way to prosecute.

Stephanie Losi: As evidence.

Cal Waits: Correct, to prosecute a crime. If a crime has been committed.

Stephanie Losi: Okay, so how would you suggest, who should the business leader really work with? As they're taking responsibility for the creation of the policy, who do they need to talk to? Who should they be liaising with, and who do they go to find out what's really needed?

Cal Waits: Right. So one is the legal department. They need to understand, based on the business that they're in, what sort of legal obligations they have. They also need to talk to their technology people to understand what technology they have in place. So understanding the assets you have, the technology you have and how then to protect it.

Those are all the people that you need to be talking to as well as even maybe someone from the outside to come in and take a look and see if you've missed anything or things like that.

Stephanie Losi: And so what would you say, once the policy's established and really procedures are somewhat in place, what is the role of rehearsals and simulations in ensuring adherence to that policy, during the actual incident?

Cal Waits: Well, there's two elements in responding to an incident. A) are the sort of tactical-level skills – the actual gathering of data and the actual maybe analyzing the log file. The large-scale rehearsals are excellent for finding where the process breaks down.

In the past, I was an EMT [emergency medical technician] and I participated in a few of what we call "mass casualty" incidents, where – generally as an EMT, you practice how to take a pulse, how to do CPR, how to splint something. Those are all skills that are necessary and you need to have. But occasionally, you want to have a big mass casualty event [rehearsal]. Where you have many people pretending to be hurt and you have multiple responding organizations, and that's when you find out a) two different departments are in two different radio frequencies, no one can talk to each other, you're taking people to the wrong hospitals, no one knows how to do a decontamination. So you really find out where the entire process itself breaks down.

So doing a large-scale rehearsal is a great way to find out that, "Okay, maybe our technical people aren't talking to our legal department, or HR doesn't know how to get involved if someone reports inappropriate material on a computer." And so having a rehearsal for that really is a way to streamline, to find out where things aren't working and to fix them, which is the point of the rehearsal.

Stephanie Losi: That's great. So you can really get kind of a bird's-eye view of "What's going on?" and, "Here are our weak points."

Cal Waits: And during a rehearsal, it's very important for there to be sort of a non-attribution policy. No one should be getting in trouble because of mistakes they made in a rehearsal. They should respond to a rehearsal in the way that they would normally respond. And if that doesn't work out, that's the whole point of the exercise.

Stephanie Losi: Right. You want to find that out before you're actually in the situation.

Cal Waits: That's right. There's no reason to be scapegoating somebody over what's found out in a rehearsal. But really to focus on areas that can be improved.

Part 2: The Complex Realities of Investigations

Stephanie Losi: Great. So I guess I want to ask you next, what obligations do business leaders have to consider their employees' privacy and other rights when conducting investigations?

Cal Waits: It may sound a little harsh, but frankly, employees shouldn't really expect a whole lot of privacy when they're using their employers' information systems. I mean, quite frankly, it's not theirs. They should conduct themselves accordingly. They ...

Stephanie Losi: And that should be in the policy as well.

Cal Waits: Right. It should be made clear to the employees what the policy is. But quite frankly, they don't have a lot of privacy, and they need to know it, and I think that might go a long way towards preventing some activities.

Stephanie Losi: And so – and how about the shareholders and other stakeholders? What obligations do business leaders have to them, again, when conducting investigations?

Cal Waits: Their obligations to stakeholders are going to be the same during an investigation as it is during any normal operation. They have a fiduciary responsibility to protect the interests of their stakeholders. One of the interesting points is that if an investigation is necessary, that's generally because someone wasn't watching out for the stakeholders' interests in the normal course of business. Whether that means a policy wasn't adhered to or someone was playing funny with the books, the investigation is a result of that and thus very important in maintaining that responsibility – looking out for their interests. They need to find out what was going on, how to prevent it in the future, and how to correct anything that may have resulted.

Stephanie Losi: Great. Because I think that is one perception that business leaders may have, is that, "Oh, if you have a big investigation, you're going to lose certain time." So I think it's important to point out that may not always be the case.

Cal Waits: That's right. But yeah, there are ways that you can conduct an investigation without impacting the flow of business. Which may be the point you're bringing up. Imaging a computer doesn't mean you have to take it completely offline for months on end. You can get an image, sort of a picture of the computer in the state it was at, and then you can take that off for analysis and either put a fresh image, or a new system, or even the current system up and running in place.

Stephanie Losi: Great.

Cal Waits: An investigation doesn't require everything else coming to a halt. There are things an investigation needs to look at. And they need to have the authority to go in and take a look, gather what evidence they need to in a way that's as fast as possible. And so that shouldn't be compromised, the way they gather information. But that doesn't always require months of or even days, necessarily, of headache.

Stephanie Losi: How can a business leader then best coordinate with law enforcement officials? Let's say an investigation does require their involvement. I know there are several situations in which that might happen. For example, if a computer security incident has a national security implication, then calling in law enforcement becomes a must. How can the business leader make that process as smooth as possible, while also protecting the business mission and interests?

Cal Waits: Right. It's important to remember that not just national security issues will require law enforcement response. I know in the United States any discovery of child pornography requires immediate law enforcement response. Also, there's a lot of incidents that you're not required to call in law enforcement right away.

In fact, a lot of companies won't call in law enforcement until they've completed their own investigation and can just sort of hand over what they've found. In fact, companies often have sort of an advantage over law enforcement when conducting an investigation. As owners of the systems, they don't need to they don't need consent to take any sort of – to gather any sort of evidence. They don't need consent to perform any sort of monitoring on their computer systems.

Similarly with national boundaries. If you have a multi-national company, and they've noticed that they've got an investigation that's going to require crossing boundaries, national boundaries they – because they own the systems, they can do the investigations in the various countries. Whereas law enforcement would have a more difficult time jumping from country to country.

Stephanie Losi: Right. Because there are different laws and different permissions.

Cal Waits: Exactly, exactly. Whereas if you own it, you can generally find out. You don't need consent.

Stephanie Losi: So what happens when things get tough? So I mean are there known or best methods for coordinating appropriate responses among all involved parties when there are more than two parties and it kind of gets increasingly complex?

Cal Waits: I mean, that's the problem with international and multi-party. If there are multiple parties in the same country, then the legal system is going to be more uniform, and that's going to be a little bit easier. When you're talking about multinational incidents, then that's the problem. Laws differ so much. Not just laws, but even just definitions of what a crime is. What may be legal to do in one country is illegal to do in another country. And so you really end up with, ...

Stephanie Losi: It's a patchwork, I mean...

Cal Waits: Yes. So it can be very difficult figuring that kind of stuff out. Trying to coordinate it all.

Stephanie Losi: And what about a situation that's unanticipated by the organization's policy and methodology? Something completely unexpected.

Cal Waits: Right. Which is going to happen. And I think in those cases, it's important to remember what a policy is. A policy is a guideline to help a company respond in a particular situation, whether that's a security policy or whether that's just sort of a standard operating procedure. But it's not meant to be some sort of rigid cage that holds you to a specific course of action when it's clearly not the way to go. So understanding sort of the letter of the law versus the spirit of the law, knowing what the policy is meant to do and meant to facilitate, the background and foundation of that policy, will allow people to respond in creative ways when something new and unexpected comes up. And I think that's where a good grounding in the technology and in what is meant – sort of educating people what you expect from them -- is a way to get the best sort of response in unexpected situations.

Stephanie Losi: Great. And are there any resources where people can learn more about this?

Cal Waits: Certainly. On the CERT website there's a section on forensics. It deals with some of the work that we're doing and points to some of the resources. If people are familiar with the virtual training environment that CERT has, there's a public library on the VTE that has a lot of forensic information, whether that's lectures, we have demos, white papers. There's a lot of information out there.

Stephanie Losi: And that's www.vte.cert.org?

Cal Waits: Correct.

Stephanie Losi: Thank you very much, Cal. This has been really good. I enjoyed learning about this, and I appreciate your time.

Cal Waits: It's been a pleasure.