Computer Forensics for Business Leaders: A Primer
Transcript

Part 1: Framing the Issue

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 Rich Nolan, who leads CERT's efforts on computer forensics. Today we'll be discussing what leaders need to know about this topic and what they can do to protect their organizations. So, Rich, let's just jump right in. I want to ask you: What is computer forensics? How would you define it, and what is its relationship to electronic evidence?

Richard Nolan: All right, well, I think for the purpose of today, it's important to frame computer forensics against what leaders and industry need to know about it, okay? So that'll be kind of our governing perspective.

Stephanie Losi: Right, exactly.

Richard Nolan: At its very core, forensics means "to bring to the forum." It's a Latin word that means "to bring to the court." Computer forensics is taking computer science knowledge and technologies and understandings and integrating them with the way that the court understands to bring this technology, this information, to the court. So traditionally, when we're talking about electronic evidence, we're talking about: How do you take a computer that has been a victim of a crime or that has facilitated a crime and gather information about those facts and formulate them in a way that the court will understand?

It's important to recognize that the technical knowledge and the technical methods that are available today may not always be acceptable in the court of law. So the court – meaning the U.S. courts in this matter – have procedures and methods and understandings for how things are admitted and what's reliable and what's not, and that has to be used in framing the electronic evidence. So there are often cases where there's technical ways of doing things, but those technical ways may not be admissible in court. So computer forensics is taking both of those disciplines, the legal aspect and the technical aspect, and bringing them together.

If you're spending hundreds of thousands of dollars on your security infrastructure, it goes to reason that you would want to be able to extrapolate information from that security information and use it in a court of law. Particularly looking at some of the current legislations like the California State Bill 1386, which some of the federal laws are being modeled after, that California Bill says that any state agency, person, or business that conducts business in California, owns or operates computerized data that includes personal information, if they should suffer a breach where unencrypted personal information is released, they have to notify the authorities, they have to notify the individuals whose data was lost, and more importantly they could be liable for damages.

So in those types of arenas, it's imperative that you have a mechanism in place that will allow you to use your security information for legal purposes to actually go after the person that have done these things, and that is what business leaders should think about.

Your return on investment is always a hard thing to codify in security, but certainly, being able to use the security systems that are in place to gather information, to make sure that the way that data is being collected, the way that data is being stored will stand up to the scrutiny of the courts.

Stephanie Losi: So what do you think are the essential components of such a mechanism?

Richard Nolan: Well, there's lots of things. The court elements are you need to have good policy in place. Within the U.S. court systems, there's two broad categories. There are issues that govern your authority to monitor and collect, and that's what you're going to be concerned with in your security policies. Do you have the proper authority, do you have the proper, um, you know, position to be doing what you're doing, to monitor and collect the things you're doing with your security tools? The second part that really affects the forensics piece is the manner in which you collect and the manner in which you store that data. The federal rules of evidence are what govern how evidence is admitted to the courts. So there are specific things in those rules that govern whether or not something is admissible or inadmissible.

One of the biggest things that will impact business leaders: There's a section that talks about regularly conducted business. The courts recognize that businesses do things that benefit them as a business. For example, cell phone companies keep track of the amount of calls you make. They know who you're calling, how long you're calling, and who's calling you. They're doing that for billing purposes. But conversely, if there is fraudulent use of a cell phone, companies can use those business records as evidence that something bad has happened.

One of the biggest things that needs to be avoided is that as an incident occurs, the last thing you want to do is, in an ad hoc manner, start getting on the keyboard and starting to try to troubleshoot it, right? That's the instinct of a lot of the admin folks. But that could introduce lots of problems. That introduces problems about the collection and the issues around the collection, and it also introduces admissibility issues because that is not part of a regularly documented procedure.

Part 2: Putting It into Practice

Stephanie Losi: So how do you communicate, if you're a business leader, how do you communicate this to your system administrators, and how do you make clear to them where is the line, like where must you stop when you notice that there may be an issue?

Richard Nolan: Well, I mean, lots of training is conducted with security administrators on how to lock down and harden and monitor systems. One of the pieces I think that is missing to complete that security triad, so to speak, is teaching people how to be first responders. So what do system and network administrators do in the normal course of business? Well, they monitor systems when there's issues, they begin to troubleshoot them, they identify the cause. Well, and technically doing that they're very proficient, but sometimes those technical methods may not always overlap with the burdens that the courts will impose upon the admissibility of evidence.

So it's my perspective that you can start off in a very secure posture that will be admissible in court, and then as incidents begin to develop you can quickly determine whether this is just a routine matter and you can de-escalate from that higher posture and begin to troubleshoot and go after the problem. But in the event that it is an issue that would require, you know, some type of

legal intervention, your initial activities as a first responder can be such that it can be easily transitioned over.

Stephanie Losi: Okay, so this is basically the principle that it's easier to step down then to step up a level of.

Richard Nolan: That's right, and sometimes you won't be able to step up. That the damage is done.

Stephanie Losi: Okay, so this seems pretty challenging, and we've talked about, you know, some routine actions. You want to make sure that if you're doing something, it's a business routine matter so you can admit it in court. What are some other challenging issues that you think leaders need to consider when they're putting a forensics program in place or dealing with an issue that turns out to be a forensics-related issue?

Richard Nolan: Well, the challenges that computer forensics present can be daunting, right? Because it requires lots of specialized equipment, lots of specialized training, and sometimes that's a hard business case to justify. But for business leaders, what they need to understand is that some of that activities belong to the law enforcement folks, not necessarily your IT staff. But what your IT staff needs to be aware of is how they can facilitate that.

So if you have a company that handles HIPAA-related information [Health Insurance Portability and Accountability Act], that falls underneath Sarbanes-Oxley, that, you know, deals with California residents and you've got credit card information or other personally identified information, part of your security plan needs to incorporate a response plan. We talk about response a lot, but what response often misses is the collection method and the forensics aspect of that, and that's where that first responder role comes in. So I think one of the challenging issues for leaders will be to get their staff trained to expand that IT policy out to include activities that first responders do so that there's a routine procedure that happens every single time.

Stephanie Losi: So you mentioned law enforcement briefly, and I'd like to talk a little bit more about that because I know this is something that maybe a business leader, you know, they don't deal with it on an everyday basis perhaps. So how do you incorporate law enforcement into your business processes so that you recognize the moment at which you need to contact them and then you can do it as just sort of a process?

Richard Nolan: Well, I mean, policy is the ultimate piece, right? I mean, policy drives everything, so in this particular instance, policy is what governs that. You want to make sure that your staff and that your IT folks understand where their limits are, understand what they should do and what they shouldn't do. I think as a general rule – and again, I'm not an attorney and this is where you would have to carefully evaluate your policies with your counsel to determine the final legal definition – but you want to stop with protecting your network, right? So if you do discover there's an incident occurring, you have a responsibility to stop the damage from occurring, stop information from leaking, you know, block that traffic, you know, protect yourself. Once that's done, then anything beyond that, I would consider falling in the realm of law enforcement. Now there are several organizations out there –

Stephanie Losi: Right, like how would you know who to contact?

Richard Nolan: Well, InfraGard is a big organization that's sponsored, I'm fairly certain, by the FBI, and they have various groups all around the country where business leaders can come and meet the FBI agents, can meet the United States Secret Service Electronic Crimes Task Force, and can

meet other folks within the law enforcement community that are responsible for investigating electronic crimes.

Stephanie Losi: So in advance of an incident.

Richard Nolan: In advance of an incident, exactly – much like your IT staff usually know who their service providers are and they talk to their upstream links all the time in normal routine matters, so when there is an incident, they already know who to call. Well, InfraGard is kind of set up to begin that same type of engagement, to let the business leaders and communities have a chance to meet the law enforcement folks so they can talk and share information. So when there is an issue or they need assistance, things are already in place to provide that.

Stephanie Losi: So what other job roles are responsible for dealing with issues of forensics from various perspectives and also making sure the business is protected in a legal proceeding – obviously it would be legal counsel, who else?

Richard Nolan: I mean, the biggest thing is that you need to understand that forensics is part of your security plan. It's part of your incident response plan. How you collect it, why you collect it, where it's stored when it's collected, all the procedural things that are in place for so many other things often are lacking when it comes to the forensics aspect of incident response. So you definitely want to have your identified chain of command. Who do you call when this happens? What are the procedures that take place? You know, having that check list, having that documented procedure in place before the incident happens, kind of shelters you and protects you from exceeding scope of authority issues. Like one of the things that often happens is in the heat of kind of responding to an incident, people often exceed their authority.

Stephanie Losi: Right, if you see the attacker you say, "Oh I need to go after and figure this out now."

Richard Nolan: That's right. I mean, what are the legal issues about recording someone's traffic on your network? Well, you need to understand what your authority to collect and monitor limits are.

Part 3: First Steps and Resource Pointers

Stephanie Losi: Okay, so you said that forensics is usually sort of an undefined area for a lot of companies. What can a business leader do to start establishing a forensics plan and a forensics capability? What are the first steps?

Richard Nolan: The first steps would be to identify: what is the sensitive data? What is it that you're trying to protect? So if a security episode did occur and in the case of a credit card company and your data was stolen and used, you want to make sure that you have methods and security systems in place that record data that is useful.

In a physical world, for example, are banks, right? Banks are really good at doing this, they've got all kind of security measures that keep your money protected, right – big vault doors that lock and that are on time-coded sequences. But they also have things that help record data in the event of a break-in. You know, countertops are very smooth because it's good for recording fingerprints, it holds fingerprints, right? Countertops are all at a same measured height. They have cameras in place. So not only do they have measures in place that prevent the loss or that money from walking out of the bank, but they also plan for, in the event if someone tries to force their way in with a bank robbery or someone tries to come in, that the procedures and methods that are in place record data that is useful for identifying that person.

So the same needs to be true for businesses that have sensitive data that they want to protect or that loss of could impose civil liabilities or criminal liabilities on them. So, in the example of a computer company in California that keeps credit card data, well, not only do they want to make sure that all the data's encrypted, that all the systems are hardened properly and they have all the monitoring tools in, but that the way that those – what is being monitored could potentially help identify who conducted the breach and, more importantly, where they came from. So just putting a lock on a door – while that's important and a critical component to everything, you also need to have measures behind that that would record what's being done once they get through that lock.

Stephanie Losi: Okay, great. So once a forensics capability really is established, how can the business leader then best support that capability, in terms of both supporting the people who are in charge of doing it, you know, your first responders on the IT team, as well as getting a buy-in from everyone across the organization so people are aware of the procedure and are willing to stick to it?

Richard Nolan: Well, I mean, it's very similar to IT policies, right? Unless you have that CEO-level buy-in, then it's very hard to implement. If password security and physical access are restricted and if you violate that there's a penalty that's incurred, well, the same thing needs to be true for that kind of computer forensics issues. They need to be rolled up into policies that are enforced by management. So the best thing you can do is give your examiners, give your first responders clear, well-defined policies that are enforced and supported by management.

Stephanie Losi: So give them somewhere to go to make sure that they can get things enforced.

Richard Nolan: That's right, and give them the proper bounds to let them do their job.

Stephanie Losi: Okay, this has been great, I really appreciate your time. I do have one more quick question, which is: where can our listeners learn more about this topic?

Richard Nolan: Oh, there's lots of places. I mean, for example, we've got several publications that are currently posted on the CERT website, "First Responders Guide to Computer Forensics," and that particular handbook is written to target the very audience to which we're talking to today. So what do system and network administrators need to know, and how do they create policies and procedures that are acceptable for court room purposes? NIST.gov has an excellent resource site for computer forensics-related issues. The FBI CART team has great resources on the web, and then of course the United States Secret Service Electronic Crimes Task Force has another great resource pool of information available.

Stephanie Losi: All right, thank you very much, Rich.

Richard Nolan: You're welcome.