CARLTON FIELDS

CF on Cyber: Leveraging the Incident Response Guide to Prepare for the CCPA

CYBERSECURITY AND PRIVACY | TECHNOLOGY | NOVEMBER 7, 2019


John E. Clabby


Joseph W. Swanson


Steven Blickensderfer

In this program, Jack Clabby, Joe Swanson and Steve Blickensderfer give practical advice on the attorneys' role in a data security incident response guide, which is a key document in preparing for California's new data privacy law, the CCPA.

Originally produced in American Bar Association Section of Litigation's Sound Advice Podcast Series

Transcript:

Jack Clabby: Welcome to the Sound Advice on incident response guides and how they can help you and your clients get ready for the California Consumer Privacy Act, which is a sort of watershed law for consumer privacy that's going to go into effect on January 1st of 2020. One of the real backbones of this is to have what your clients or companies you work with as lawyers would call an incident response guide or an incident response plan. This is a really usable document that tells you who in the organization responds to data loss events or data loss incidents.

We've got with us here quite a bit of talent on the cyber security side, all active members of the American Bar Association. We've got Joe Swanson from Carlton Fields in Tampa, Florida who leads the cyber security and data privacy practice group at the firm. Joe, welcome and thank you.

Joe Swanson: Thank you.

Jack Clabby: We've also got Steve Blickensderfer who's very active in the ABA as well as in the Florida bar in our Miami office and does quite a bit of privacy work. So, Steve Blickensderfer, thanks so much for joining us here. And I am Jack Clabby, a former federal cyber prosecutor also at Carlton Fields with Joe and Steve. I do a lot of work with boards of directors and companies on incident response and incident management.

So, the acronym that we sometimes use for incident response guides is PIN, P-I-N. P is preservation, I is investigation, and N is notice or notification. And so when you are working with clients to put together their incident response guides or to look at it again in preparation for California's new law, keep these three things in mind.

I'll get off right on the first bat to talk about preservation, which is the P of PIN. What does preservation mean? It means when you begin your incident response guide, you're going to be doing a lot of effort within the systems of the company. But it's important, particularly as lawyers who have a piece of this process, to preserve the evidence of the event. And that might mean when you take computers offline things could get destroyed. So, working with the IT and information security professionals at the company, working with the third party forensic investigators, and working with the general counsel's office to be deliberative and thoughtful about how changes to the system to investigate, mitigate, and contain the cyber security incident, what impact that has on the evidence that's retained. It's really important if there's going to be litigation, if there's going to be an attorney general or similar regulatory inquiry to have a good record of what occurred. This is something that the lawyers can really influence and that the IT and information security professionals don't often have front of mind.

Alright. So, that's the P. Joe, can you talk to us about the I in the P-I-N concept?

Joe Swanson: Sure. I in this acronym stands for Investigate. And here you also are going to need a multi-disciplinary approach with your legal team, both general counsel and as needed outside counsel, the forensic team and the internal information technology and security assets to investigate the matter. What happened? Is it ongoing? And, a key consideration here is attorney/client privilege. This is a portion of the work stream that can involve very candid assessments about what has happened and why it happened. And those candid assessments may not be very flattering for the organization and so therefore the organization by having their general counsel's office and as needed outside counsel involved can try to maximize the extent to which that work would be covered by the attorney/client and possibly work product privilege. When you're executing on the incident response guide, you also want to have the exhibit or appendix at the back that has a roster of all of the internal and external assets that will be called upon to investigate, so that's the forensic firm, outside counsel, the insurance agency and broker so that those can be notified and involved in the investigation as quickly as possible.

And then finally, just be cognizant of what kinds of documents are being created in this phase of the response because, again, they may contain very candid assessments. They may contain assessments that turn out to be wrong as the investigation unfolds. And so this may be an area where oral briefings are preferred to anything written until more is known.

Jack Clabby: Alright. Thanks, Joe! So, we've talked about the lawyer's role in the preservation concept within the incident response plan. Now we've talked about the lawyer's role in the investigation concept in this P-I-N method. Steve, can you help us explain, what is the role of the attorney in the notification or notice part of PIN as a guide to your incident response plan?

Steve Blickensderfer: Sure. Thanks, Jack! So, not every incident rises to the level of a breach that needs to be noticed as anticipated by the 50 state breach notification laws. And so the attorney's role at the end stage of PIN, Notification, is to determine what, if any, notification is required both internally, the notification process and procedure for notifying affected departments or assets of the business, the external notification procedures with vendors and those who are doing the triage and the efforts to contain and prevent the incident from escalating, and also the external communications to the affected individuals whose data may have been compromised to the press and the media. And so what the notification procedures aspect of the process will look like is going through almost a checklist of questions based on an analysis and what these 50 state breach notification laws look for. Where are they? And this will start with where are the consumers located will be one question so that you know which laws to look for and to analyze. And this will be kind of part of the whole risk process in which is, is there a risk of harm? Because a lot of these statutes will base whether or not notice is even required if there is a risk of harm based on the incident and exposure of the personal information.

Increasingly, some of these statutes are basing notice to, also may require notice to the attorney generals of the various states or the regulator who's in charge of the maybe consumer affairs department of the AG's office. There are some that require, some states require notice to law enforcement as a, you know, matter of course. And there may also be required notice to third party vendors. That also may be required by contract, separate and apart from any laws. So the lawyer's role will also be to examine service provider or vendor contracts to determine what, if any, breach or incident reporting notice obligations the business has. And increasingly we're seeing a trend where vendor agreements are being modified to discuss and anticipate and prepare for incidents and to lay down really stringent notice, you know, obligations on the business in some instances. So, understanding and basically going through that part of the process, the N, is notifying not just the affected consumers if possible but many other aspects and in some cases regulators. Laws are being updated and changed to include the insurance regulators or, you know. Banking and healthcare, they have their separate HIPPA and Gramm-Leach-Bliley Act notice obligations. There's also if credit cards are involved the PCIDSS has a whole separate procedure.

But, so to wrap all that up, the N in Notification stands for this entire process of who you tell, what do you say because many of these laws require or the contract with the vendor require certain disclosures to be made. And that's all at the end process.

Jack Clabby: Thanks so much, Steve! So, this has been me, Jack Clabby, from Carlton Fields with my colleagues Jow Swanson and Steve Blickensderfer. We've been talking about the P-I-N method for evaluating a lawyer's role in the incident response guide. We're all going to be doing this a lot in the next few weeks getting ready for the California Consumer Privacy Act. So, thank you Joe, and thank you Steve.

Steve Blickensderfer: Thank you.

Jack Clabby: If you'd like more information on anything we've talked about, get in touch with any of us. We're at carltonfields.com. Got a pretty good privacy page set up with a lot of resources and ways to get in touch with us. Thank you.