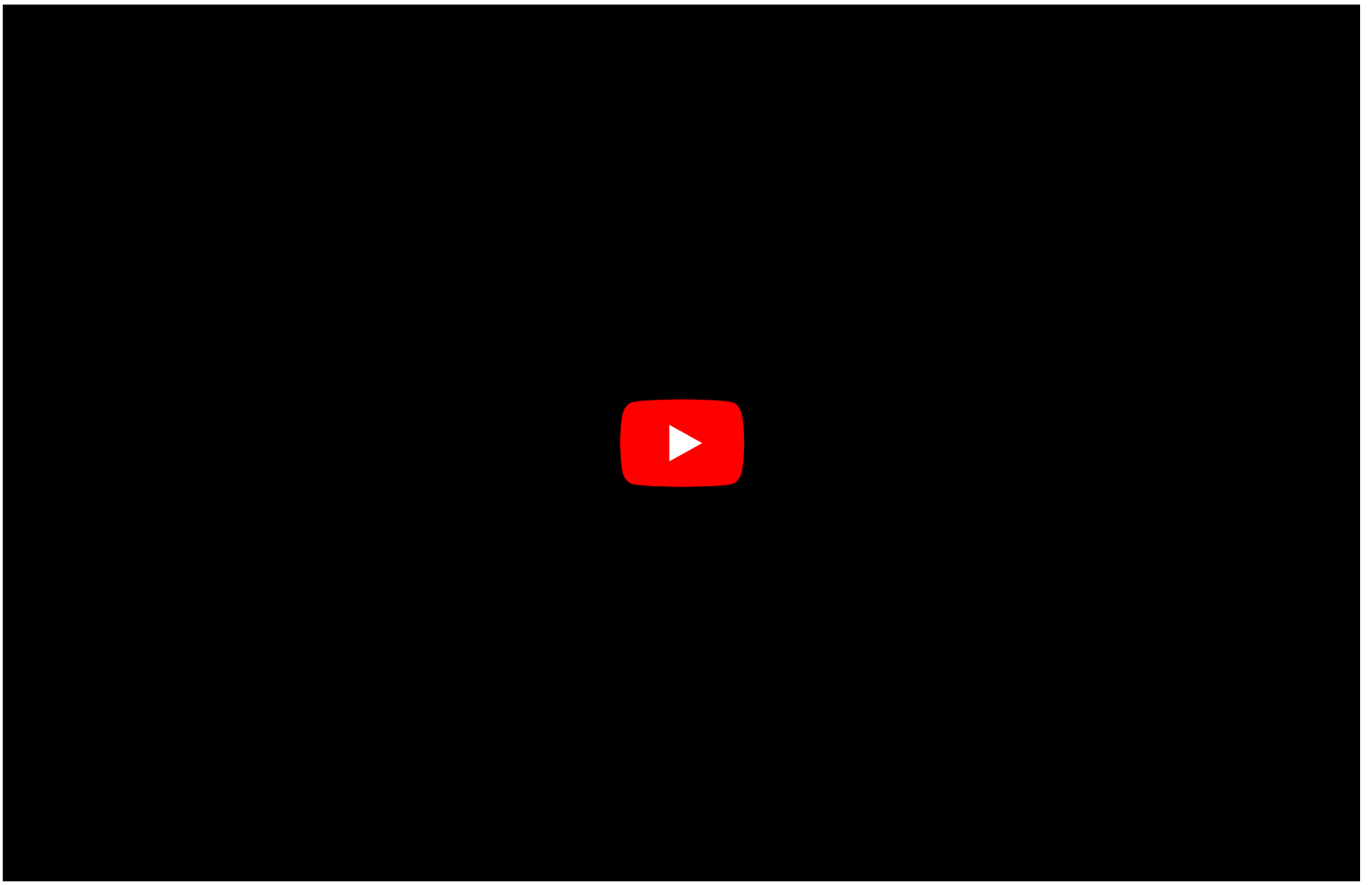
CARLTON FIELDS

CF on Cyber: Deep Dive into the DOJ's Guidance for Cyber Best Practices

October 30, 2018



{^youtubevideo|(width)640|(height)480|(rel)False|(autoplay)False|(fs)True|(url)^}
In Carlton Fields' latest *CF on Cyber* podcast series, **Jack Clabby** and **Joe Swanson** discuss the latest guidelines released by the Department of Justice Cybersecurity Unit, which provides

recommendations to companies about how to prepare for and respond to data security incidents. The guidance, which updates the original guidelines issued in 2015, details best practices in several key areas: steps to take before a cyberintrusion or attack, incident response, and what to do after a cyber incident.

Businesses, as well as lawyers, will benefit from the insights provided in this podcast. Both Jack and Joe are former federal cyber prosecutors who represent companies in investigating and responding to data security incidents.

Read: Best Practices for Victim Response and Reporting of Cyber Incidents, Version 2.0

Joe: This is Joe Swanson. I'm joined today by my colleague Jack Clabby. We're going to talk about the DOJ Cyber Security Unit, which recently released guidance for how to prepare for and respond to data security incidents. This was a revised guidance that was originally released in 2015 but has been beefed up since it was originally promulgated. We love this stuff. Jack and I are both former federal cyber prosecutors. I was a cyber prosecutor here in Tampa, Jack in New Jersey. And so what we want to do today is walk through the guidance and where appropriate add some color based on our experiences, both as federal prosecutors and then over the last several of years, in private practice. Without further ado, I'll hand it over to Jack.

Jack: Thanks Joe. So, we're talking about best practices for victim response and reporting of cyber incidents, this is version 2.0. As you said, this has certainly been beefed up since 1.0, which came out in 2015. I like to think that I've also been beefed up since 2015, that's because I have been hitting the weights. We'll be talking a bit about four things - there are four subsections of this guidance. The first is steps to take before a cyber-intrusion or an attack, the second and third are related to incident response itself, and then the fourth is what to do after a cyber incident.

So, I think the take away is for at least small business and mid-size business, comes in the first section, steps to take before a cyber intrusion. There's about 10 tips, they're all pretty good, it's one of those things where it seems like it's intuitive and everyone should know it, but if you didn't look at it written out this way a lot of this you might miss. The first is, probably the best place to start, which is educate senior management about the threat. There's some good tips in here about how to do that, and get buy-in from executives. The second is identifying your crown jewels. Now that is something, Joe, that we've always talked to our clients about, we call that risk mapping. The third is to have an actionable plan in place now. I think this advice is a little bit incomplete - it's one thing to have a plan, it's another thing to have a plan and train against it. What have you seen representing clients about the risks and rewards of that?

Joe: The plan is only effective if it's tailored to the organization. It's fine to start with a template that an organization might find on the internet. But it really ought to be then tailored to that organization

size, its industry and what you just talked about, the risk profile that it has and what its crown jewels are, which may vary from organization to organization. It then is only effective if people are aware that that plan exists and that they have trained on it. Because what we have seen, time and again, is organizations will have a plan but they haven't practiced with it. So, one, it's not effective, and two, if there is any litigation or some type of regulatory inquiry, the presence of a plan that was not followed can actually be more problematic than if there was no plan to begin with.

Jack: So the best place to be is to have a plan, train on it, follow it. Then probably better than that is to have no plan at all.

Joe: That is exactly right.

Jack: At least no written plan. The worst place to be is to have a plan, and which you are acknowledging to future litigants, hey I knew what I was supposed to do.

Joe: Right.

Jack: And then you don't follow it.

Joe: Exactly, because then that will be the yard stick against which your organization is measured.

Jack: That is bad deposition exhibit one in a data breach class action. The fourth tip here from the Department of Justice, in their best practice and guidance, is to engage with law enforcement before an incident. If you're planning a party and you're in high school do you go up to the police beforehand and say, you're about to have a bunch of underage kids drinking in your house? Not really, right? But I think law enforcement is sophisticated enough to know that breaches are going to happen. In practice, what does this look like? Do you just call the sheriff's office and have him come over to your business?

Joe: It can be one of a number of things. On a federal level, the two primary agencies that are tasked with this are the Secret Service and the FBI. The Secret Service has done a great job reaching out to the communities in each of the cities where they have a field office. Through what they call the ECTF, or the Electronic Crimes Task Force, they hold quarterly meetings where they bring together members of the community to educate them on current threats. It's a great way to know your local Secret Service agent. Another similar option is with the FBI through their InfraGard program, which one disseminates information about threats that they are seeing to members of the community. They also hold periodic meetings, and what's nice about either of those is that invariably there will be local law enforcement present at those meetings, which means if you attend them, you can not only meet the Secret Service or the FBI, but you'll also get to know your local Sheriff's Office or your local police department which increasingly have cyber units of their own. And the sophistication of those

units varies by jurisdiction. But bottom line is it really behooves an organization to have a phone number for someone in law enforcement or to make sure that their outside council does.

Jack: This is real, like this is a real thing that the FBI and the Secret Service and Homeland Security will do. And they want to do it. A year ago, we did a panel with an FBI cyber agent in Atlanta and he reached out to us afterwards and said, are there clients who want to have interaction with us. And I think he ended up reaching out (you know there's no preferences here), but he reached out to a bunch of the local insurance companies who are operating in the Atlanta area, connected with their cyber underwriters and claims folks, and met a bunch of the companies that had real risk. And so this is not something that just looks good on paper – the FBI, the Secret Service, and Homeland Security will actually do this. And folks who are listening to this should pursue those opportunities in the cities that they're in. It really does help to know. Now the fifth piece of guidance that the DOJ provides is to have appropriate workplace policies in place. You know it's hard to say what's appropriate, but Joe, does the DOJ give some examples of what these might look like?

Joe: They do, Jack. The examples they give are to integrate incident response into personnel training, which would mean as you onboard your personnel and also on a periodic basis thereafter, work with them on incident response so that everyone is familiar with it. The other example they give is to promptly revoke computer credentials of terminated employees. Often these incidents are perpetrated by insiders and it's a very good idea as this guidance reminds readers to revoke computer credentials of terminated employees who may otherwise be inclined to take some adverse action against their organization.

Jack: And I had a couple of cases at the U.S. Attorney's office where there was an insider threat and in one of those instances it was an insider who believed that he or she was going to get terminated and sort of was sucking up everything she possibly could, or he possibly could, on the way out. And we've seen this in private practice too where you have a savvy technology employee who believes that a cut is coming or is about to go to a competitor. And having the right sort of controls in place as that person exits can be the difference between keeping the crown jewels and losing them. The sixth piece of guidance that the DOJ offers, as to prevention, is for companies to institute basic cyber security procedures. And it is still shocking even which sophisticated larger companies, even larger public companies who we work with, have some of the three or four basic principles that are put out and the guidance are not followed here. Joe, what are some of those principles?

Joe: Yeah, those principles include having a reasonable patch management program, making sure that your software and networks are patched regularly. Two, ensuring that there are access controls in terms of who has access to what on the network and the principle of least privilege, network segmentation, so that if there is some sort of a compromise, the perpetrator is not able to just roam through the organization's networks, and multifactor authentication, which is, you know, more

commonly known as two factor authentication, anyone who's done online banking would be familiar what that is.

Jack: Multi-factor authentication being particularly important to stop what we've seen in the, what, six or seven months here. These Office 365 e-mail hacks where the bad guys are using the ability for even employees who only work at desks to log on to these systems remotely.

Joe: That's right.

Jack: You know this is two things. It's the policy of least privilege, right? Why do you give desk employees the ability to log in remotely? They've never done it in 10 years of employment. And two, multi-factor authentication, you can't use a password found on the Yahoo data breach website, you know, the Dark Web, to just go and hack employees' e-mail from a remote point of view. The seventh piece of guidance here of the 10 best practices that the DOJ's guidance offers is to procure appropriate cyber security technology and services before an incident occurs. There's a couple pieces to that. One is *appropriate*, right? What's appropriate? You know, if I'm reading a first draft of a brief and the word appropriate fills in from an associate, I will usually take the word *appropriate*, circle it, and say what do you mean by this, right?

Joe: Right, right.

Jack: So appropriate, it's careful. The second thing is before an incident occurs. So what's appropriate is going to depend on the company itself, what its risk profile is, and what it can afford, frankly.

Joe: Sure.

Jack: And how quickly it's going to need to respond. But why is it important to do all this, Joe, before an incident occurs?

Joe: Because if it's after an incident, that's when you want to be executing on your incident response guide and you want to have all your pieces in place to handle that incident as smoothly as you can. And the way that you can position yourself best is to have lined up these services ahead of time when you can negotiate rates, when you can get in place the requisite engagement agreements, and what we would like to see is clients having incident response guides that have two lists attached to them. One is a list of the internal resources that will be called upon in the event of an incident, and the other is a list of the outside resources that will be called upon. And particularly with regard to the outside resources, if an organization has cyber insurance, they would be well served checking with their broker or even the carrier to make sure that their list of outside resources is preapproved by the

carrier so that if they do call upon that forensic firm or that law firm, all of those charges are going to be approved.

Jack: So the eighth piece of guidance here that the Department of Justice is giving for steps to take before a cyber-intrusion or a hack, is to have appropriate authorization in place to permit network monitoring. This idea is, what can a company do to observe the inputs and outputs for each of their employees. And I think, you know, up to this point the DOJ guidance is user friendly for any business person. It gets pretty hairy here talking about specific statutes, and frankly, when I read this I was a little scared - are there things we're doing either in our own firm or that we're telling clients to do that would violate the federal wiretapping statute? I mean that's nuts. I get the feeling that maybe this part of the DOJ guidance was written by someone different than the rest of it.

Joe: It may very well have been and I agree with you that it stands out whereas most of the document is very, very accessible. This one is a bit more dense, and the subject matter is a bit more sobering, but really the takeaway from it is this: have some type of authorization in place that allows the organization to permit network monitoring because that will be helpful from both a detection and a response standpoint. And what it may boil down to is just having a solid user agreement that you have employees sign when they join the organization and that you have them affirm, on an annual or some other periodic basis. That can go a long way here and should allay the concerns raised by that portion of the guidance.

Jack: And we write these for clients, really what it is, is you want to make it plain language. You want it to be: we're a company, you're using our resources, you're connecting devices to our network. We're going to watch what you do to protect the company. We're not watching it to embarrass you. We're not watching it for other purposes. We're watching it because we want to make sure that the stuff that comes in and out is good and clean and if there's a problem, we want to be able to trace it back.

I think plain language in those user agreements is important. But for companies that are just starting out on this step, this shouldn't be an intimidation. If you're reading the DOJ guidance here for, if you're finding out what to do, jump in, get a user agreement up and running and be candid with your employees about what you're going to do.

The ninth piece of guidance that the Department of Justice is providing for prevention gives a little shout-out to folks like you and I, Joe. This is to ensure your legal counsel is familiar with technology and cyber incident management. And those are two different things too because a lot of people know about computers, but don't necessarily know about cyber incident management. In the same way that the chief technology officer or the chief information officer of a company knows about how to buy printers and how to buy hardware, but is different both in function and skillset than the chief information security officer. How does this come up in our practice, Joe?

Joe: So where this comes up is both for internal referrals and external referrals. The point being that for privacy and cyber security preparedness and response, you really want a practitioner who is familiar with that field. And it typically can be someone within your firm who's developed that practice, or even from another firm can just come in on a one-off basis, this is an area where you do want experience, people who have law enforcement contacts can be very, very useful here. A good analogy is a commercial lease. You don't want someone doing it for their first time.

Jack: This is true too for the lawyers who are listening to this. If this is not an area where you specialize and one of your clients has an incident, you should prepare in advance. Who are you going to refer that to? And what are the terms of that referral going to be? Are you going to get the client back after you make the referral? But that's certainly something; you don't want to be over your head on this. You know, what we do, we do and we don't do a lot of other things. And this is an area where, you know, sometimes these engagements are 24 hours long. You get in, you solve the problem, and you're out. You don't want something that if it's handled correctly can last 24 hours to end up lasting 24 months…

Joe: That's right.

Jack: …because of problems at the outset. The tenth and final recommendation from the DOJ, at least on prevention side, is to establish relationships with public and private cyber information sharing and analysis organizations. Now, what are these? There's a couple. There's some public information sharing organizations. Many of them are under the FBI or Homeland Security. And then there are some private-side ones where there's information sharing. The DOJ guidance has some references to antitrust law here. Again, it's all very scary and to some degree intimidating. This is really only useful for who, Joe? I mean is this, are small organizations going to get a lot of benefit from this?

Joe: Well, the formal information sharing and analysis organizations, the ISAOs or the ISACs, are really going to be most useful for larger organizations and when it comes to ISACs, really for larger organizations that are in one of a dozen or so critical infrastructure industries. Outside of that, however, there really can be some benefits for our organization regardless of its size from information sharing, and that can also mean just using some great publicly available resources that the federal government has put out. And two things that we like to point our clients to are US-CERT, which is a compendium or a website maintained by the Department of Homeland Security that contains all kinds of resources, instant response guides, templates, those sorts of things. Also the Small Business Administration has great resources. We commend each of those to clients, or potential clients, particularly if they are small to medium size organizations.

Jack: On the private side, you know, who sees the most of these breaches are probably insurance carriers and the brokers. Another good source of information on what is happening in the industry is

talking to your brokers or to your carriers about what's going on for companies that are affected by this. If you have a commercial banker for your company, that's also someone good to about because they see inflows and outflows of money and if there are things that are happening across their purview, it's worth getting know them. But think broadly in terms of who you can draw information from and the important thing is all this stuff is free.

Joe: Mm-hmm.

Jack: There's both the private information sharing organizations you're talking about and talking to your brokers and your carriers, things that are either free or things you're already paying for.

Joe: That's right. So the next portion in the guidance after those 10 steps that it identifies for cyber intrusion preparation is how to respond to a cyber-incident. And what this means is how execute on your incident response plan. And there are number of steps identified in the guidance. We're going to walk through each of those, just as we did the last section. So Jack, step one is make an initial assessment. It then identifies a couple of components under that task: data collection and working with incident response firms. Now as you reviewed this guidance, did anything stand out to you as really not being addressed in the guidance?

Jack: That's right. So for sophisticated entities that are having real breaches, or even for smaller entities that have had sensitive information taken, a lot of risk flows from that information coming out. They'll need to notify often the consumers whose information are at risk, and also, they may need to notify a regulator or at least a state attorney general's office. Real liability can come from it and so at the outset any incident response guide for really sensitive information or potentially a risk to the business should involve the guidance of their lawyers. And it's not simply because that's what we do, Joe, although that's part of it, but it's also because this is a, or it can be a, privileged investigation into something that went wrong at the company that is done in the shadow of legal liability. And as a result, there's a possibility that it can covered by the attorney-client privilege and the work-product protection.

Now, is that just a sort of cover-your-rear? Well, it can be described that way. But the real benefit from it is if there's a lawyer in the room and there's some veneer of privilege, it allows people to be more honest and straightforward and it lets the investigation into what is happening and what went on happen more rapidly without folks putting up as much of a barrier as it can be. So I think there's a practical reason to involve a lawyer at least for a sensitive breach at the outset. And I think the DOJ guidance, while useful from a technical standpoint, doesn't take into account that the interests of a company responding to a breach are not the same as the interests of the DOJ. The DOJ is a law enforcement entity who wants access to all the data and the information because they're trying to catch the bad guys. So that's a real contrast that I think as companies review the DOJ guidance, they need to think about.

Joe: That's a great point, Jack, and I wanted to stay on that topic a bit longer, this notion that the guidance may not necessarily always align with the interests of the organization. That said, in my view, when you read the guidance, there certainly are plenty of instances where it aligns very much so and in one of the steps the DOJ identifies, which is to record and collect information, which is something they talk about after implementing measures to minimize or mitigate the damage. On this recording and collecting information, do you see the interests of the organization there, Jack, aligning with law enforcement? And if so, how is that?

Jack: I think that's exactly right. So that's one area where DOJ's desire to have evidence of the crime of which the company is the victim is aligned with the company's interest in knowing what happened and being able to prove later what occurred. And this is an area where I think there's some good guidance here from the Department of Justice about how to do this. Litigation readiness and defending to a regulator what occurred at the company also allows law enforcement to find out who did this and to pursue them. Now, law enforcement has traditionally been criticized for not being able to do enough against nation state actors who might perpetrate these larger incidents, but I think in the last three to five years they've had some indictments of foreign nationals and look, it's on everyone's mind, I mean, one of the, the sort of unusual silver linings to our national conversation about what Russia is doing or not doing with their special elections has been a conversation about what U.S. law enforcement's ability is to protect in the homeland, I guess you describe it, our borders.

So, here's the point, right? There's three steps at the outset before notification that the DOJ identifies. Step one is triage concept, step two mitigation concept and step three the preservation concept. They don't happen in order. And that's the piece that is a little bit of concerning. I think that whoever technically is doing the triaging at step one needs to have preservation also on their mind because frankly, turning on or turning off a machine can mess with the preservation. So I would reverse those steps. I would probably have it start with preservation, then I'd have triage second, and I'd have mitigation third. But good training on that incident response guide can make sure that the technical staff who's involved in the triage and mitigation understand the importance of preservation.

Joe: The good news is that, regardless of which order you take those steps, an organization thinking about those steps is also going to be thinking about things that may ultimately prove useful for prosecution and interaction with law enforcement, and so in that regard the guidance really reinforces the things that organizations should be thinking about. The next step that they identify, and that those earlier steps really lead up to, Jack, is notification and, and you know, certainly that includes people within the organization that should be those you've identified in your incident response guide as being part of the team. It may also depend on the nature of the incident in terms of who you get involved at the organization. They also talk about federal responders and of course because it's a DOJ document, they spend quite a bit of time on, on the virtues of contacting law enforcement and both as prosecutors and in private practice we certainly are well aware of those

virtues. But it may be a bit more of a complicated analysis for an organization dealing with an actual incident. What are some of the benefits to contacting law enforcement that, you know, you and your clients think through, Jack, as you're evaluating whether and when to reach out to them.

Jack: Right. I think if you read the DOJ guidance, it's assumed and presumed that every time there's an incident, you're going to contact law enforcement. And that's not true for a couple reasons, right? Or it's not in the interest of the company. I think first, some smaller incidents, there's just no reason to, there's no loss. There's an incident, you may have to make notification to consumers, but it's not the sort of thing that law enforcement gets concerned about. But let's think about pros and cons for this for a bit – if there is a larger incident that is clearly the result of a criminal act as opposed to a lost laptop, alright? There's a crime that's been committed and the public resources are available to assist. In some cases, making a report to law enforcement early can make the company look better because law enforcement one, is in fact helping mitigate the risk, but two, it sends the message that the organization can't be bribed, that the organization can't be ransomed and that it's going to go to law enforcement every time and I think that's a real deterrent effect particularly for organizations that receive targeted attacks. Additionally, in some instances, involvement of law enforcement particularly early can actually help catch the bad guy. And in some instances if it's in the first 24 to 48 hours, usually, of a diversion of payment, involving law enforcement can actually recover the money that was lost. Under most states' data breach statutes, if a company has to notify the consumers, you can get up to 15 days of law enforcement approved delay in making that notification, which can be important in a large data breach if you need more time as a company to figure out who was impacted. And I think lastly, for companies that have a public perception, the real risk isn't so much not notifying law enforcement, it's later on, having someone find out that there was a crime committed and you didn't call law enforcement. That makes you look bad, right? So, to highlight the pros, they can sometimes help, it makes you look good, you can catch the bad guys sometimes and deter crimes, and not doing it and having it come out later makes you look bad. Now the cons are pretty well known too, right? The biggest is, I think there's this fear that opening up your files or your service to law enforcement during a hack will turn their attention on the company and the company will find itself more likely to be prosecuted. In our practice both as assistant U.S. attorneys and then in doing this in private practice now for four years, my view on that is that it's simply not a risk that's a real one. Now I'm sure that there's outliers, but we've done dozen of these and we've never seen it.

Joe: That's right.

Jack: Fullstop…

Joe: That's right.

Jack: Now law enforcement may have different goals, they may be disruptive, they may want server access at a time when you don't want to give it to them. And there is the remote possibility that if

you're running a regime that's fraudulent, then you probably shouldn't call the police, right? But, but we haven't encountered that yet. I think the biggest thing is how do you handle this from a logistics standpoint and I think the one real tip that we found is the best is you have one person in your organization during the breach who is the single point of contact for law enforcement and can make decisions on the fly about what to give and what not to give to law enforcement. It's having one person, being accountable, making sure they're the only person talking back and forth with law enforcement and that they're equipped with the authorization to make decisions. I think if you have that single point of contact who can say yes and no, you're more likely to get through this without trouble.

Joe: Well, this issue should be spelled out or at least have a placeholder in the incident response guide and that person, whether it's an inside employee or outside counsel, identified as being the point person for any communication with law enforcement. And of course if you have cultivated a relationship with law enforcement ahead of time, that may make this calculus that much easier when you're actually faced with it. The other two constituencies that they talk about in the guidance for possible notification are the regulators, and we've talked a bit about that here. And the guidance really says that the specifics there beyond the scope of that document and then other potential victims. After it goes through, Jack, the different ways in which to respond to a cyber-incident, it actually stops and says what not to do following a cyber-incident. And it's a shorter piece but it's an important piece of the guidance. What are the two major takeaways from that section?

Jack: That's good. One is a warning, the other is, well I guess they're both warnings of form, right? The first is don't use the compromised system to communicate. And the second is do not hack into or damage another network. Now as to the first, using a compromised system to communicate, it has happened where clients have emailed us, hey Jack or hey Joe, we think our email system has been compromised. And what's the problem with that? They're using the potentially compromised e-mail system to communicate with us! So first thing's first, and your incident response guide should have this, what are the alternate methods of communication? Now I know, because our offices are right next to our information security officer. We keep fully charged radios, handheld radios, in case things really, really go down, we have radio backup, but you know there's a lot web-based communication tools…

Joe: Sure.

Jack: …that companies can use. And frankly just using a phone is reasonable. It's most likely it'll be a compromised email or a compromised server. The second piece is don't hack into a damaged network. This is the DOJ reading the Riot Act. Look, sometimes companies will, usually it's not within the company, but they'll often hire smaller incident response shops who are probably pretty good at hacking and maybe what they do to keep the lights on is they'll do these penetration tests where they're hacking companies for good, and it's very tempting if you give a person like that a budget and

you bring him in, and he knows who the bad actor is, for him to say look, you know I can put a little piece of script on that guy's systems and, and we can show him that we're not to be screwed with. That is illegal. You can't do it. And the DOJ is saying as much. So, I think that's clear and think we're going to see some hack back prosecutions probably coming soon that might be something that the DOJ's signaling here. What are the next steps here? So the last piece of guidance they leave for us in this DOJ best practices guide is what we might call a post-mortem, you know, what to do after the cyber incident is over. After you've done your triage, your mitigation, your preservation, and your notifications what, what's left, Joe?

Joe: Sure. The points that the guidance makes and, and we endorse these full-throatedly, are one, remain vigilant. In our experience, you put out one fire and quite often it's smoldering somewhere else because the perpetrator has done more than one thing to your network or has gone in to do one type of an attack and then, you know, leaves ransomware on their way out the door. So, no one should have a false sense of security, they should remain vigilant until they've ensured that all the fires are put out. Two, address the shortcomings that will invariably have been identified in the course of responding to an incident. And that can mean, how did the incident response plan function, how did the team work, were there members of the team who didn't do a good job, were there members of the organization who should have been present that were not, what can we do to make this go better next time, and, and that's important for a couple of reasons. One, there in all likelihood will be a next time and this is real missed opportunity if an organization does not stop and take stock of how things went and how they can be improved. And two, just from a liability standpoint, because there is likely to be a next time, if that next time occurs because an organization failed to address shortcomings identified in incident one, that is going to be a glaring red flag for anyone looking to criticize the organization after there is a subsequent incident.

So Jack, we've walked through the document and its four sections or so. We wanted to just end here with a few takeaways. You know, at a high level, I think the document is a good refresher on incident preparation and response. Would you say it's a one-stop shop or is more of a kind of a checklist or a supplement for organizations to use as they prepare for cyber security incidents?

Jack: I think it's a primary source that can be used to help a company with an existing incident response plan improve it, ask some questions about it, and test it. So the best use of this is, have your chief information security officer or your general counsel, whoever handles your risk, take out the incident response guide and then take out this new DOJ guide to put them side by side and as the reviewer walks through the DOJ guide, see if the issues that it addresses are present in the incident response guide. Now some of the preventative tips won't be in some of them – the idea of having the right computer user agreement in place to monitor systems, that isn't in the incident response guide, but that, I think, is the concept. This is a primary source document that you'd have open while a company is reviewing its incident response guide to see if everything's either covered by that incident response plan or elsewhere in the company's policies and procedures. There is a lot

that's good about what it says, its emphasis on the policy of least privilege, patch management, two factor authentication. Those sound like common sense now, but companies are still making those mistakes. The idea about lining up service providers ahead of time, and frankly, calling them and telling them, hey, you know, Joe, you're our guy, we're going to call you, it might be in the middle of the night, just get ready for that so you know it's us. And then the idea of conducting a post-mortem after the dust settles. I mean, these are all things that incident response guides should have some coverage for and I think using this guidance that way would be, I think its best and most successful use. What it probably isn't good for is if a company is starting from scratch, the better federal resources are the non-law enforcement resources. It's things like US-CERT's offerings. The Small Business Administration has a good website with some incident response and risk management resources. Now I think those are better places to look for a company that's just getting out. Anything else that you see, Joe, that you think would be good to keep in mind?

Joe: I would just really like to acknowledge and thank DOJ, that throughout this document they refer to organizations as victims. That aligns with all of the public pronouncements that DOJ, whether it's FBI leadership or the U.S. attorney's offices, are communicating and it really, I think, underscores their view of organizations as victims, as entities that are to be worked with and to be partners in this effort to both combat and respond to these incidents. And so I think that's meaningful in this document and DOJ is to be commended for that.

Jack: On page 22, I think this a good quote, when they're talking about notification of other potential victims they call them other potential victims. If a victim organization uncovers evidence of additional victims while it's responding to a cyber-incident, it should consider promptly notifying the other presumed victims. I mean they're going out of their way to make this point.

Joe: Exactly. And again, this is not an aberration – that's a message they stress in all of their other communications and I think that's a real good bit of news for businesses and other organizations throughout the United States.

Jack: So, this is Jack Clabby from Carlton Fields.

Joe: And Joe Swanson. And we thank you for listening to us.

Presented By

John E. Clabby

Related Practices

Cybersecurity and Privacy