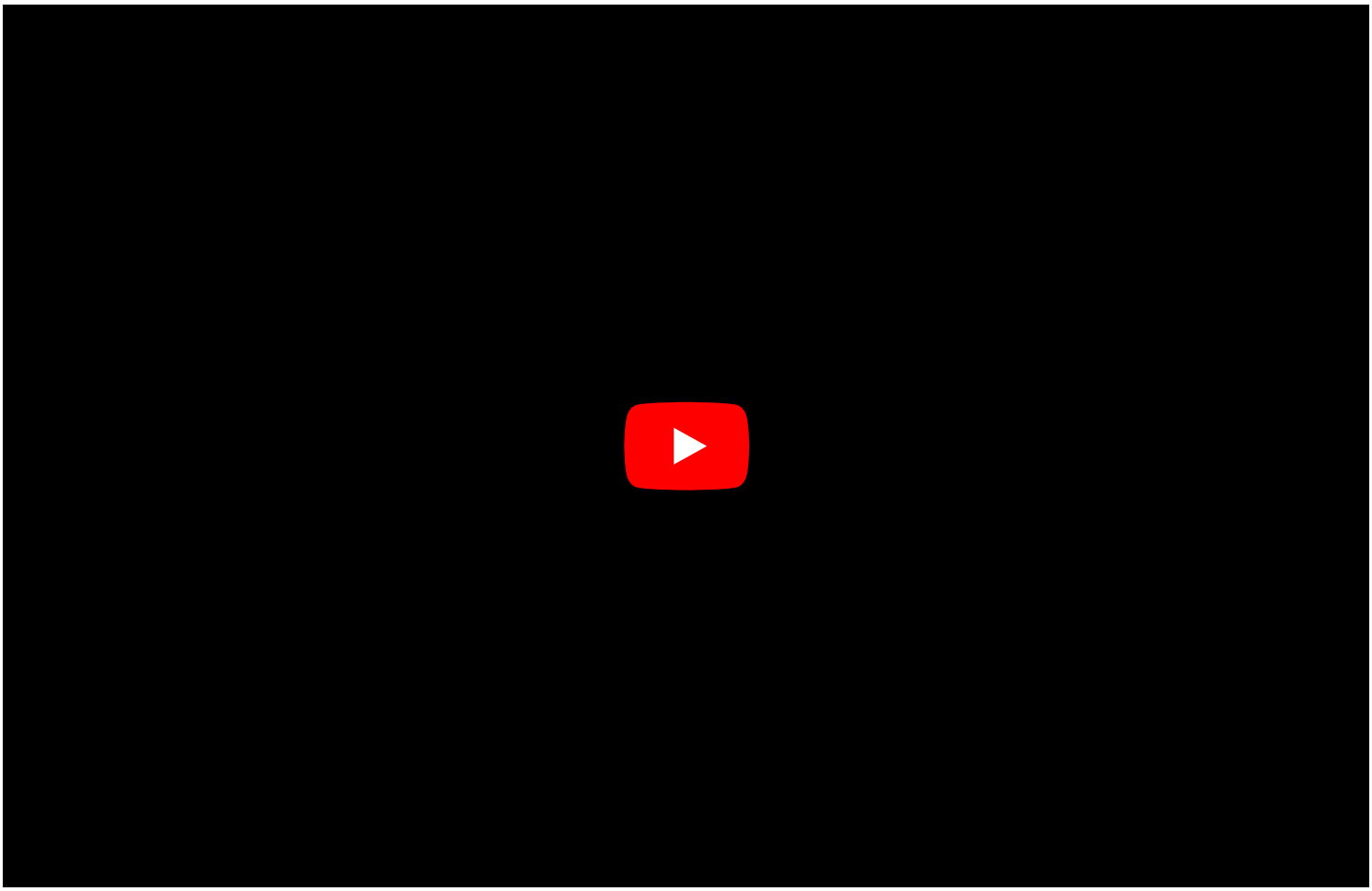
CARLTON FIELDS

CF on Cyber & FICPA presents Refeathering the Pillow: Catching, Containing & Cleaning up Cyber Fraud

October 04, 2019



In this podcast, cybersecurity attorney Jack Clabby discusses safety and risk management in data loss incidents with Mia Thomas, CPA, CGMA, Director of Learning for the FICPA.

Transcript:

Mia Thomas: Thank you for joining us on today's podcast. Today we will talk about Refeathering the Pillow: Case Studies in Catching, Containing and Cleaning up Cyber Fraud. Symantec's 2019 Internet Security Threat reported that there is an average of 4,800 websites compromised each month. Now, that's each month, not quarter or year, but each month - 4,800. Craziness, right? Well, also ransomware shifted targets from consumers to enterprises where infections rose 12% from last year. With us today we have Jack Clabby, an attorney and shareholder at the law firm of Carlton Fields. Jack, thank you so much for being with us on our podcast.

Jack Clabby: Thank you so much for having today, Mia.

Mia Thomas: Well, Jack, tell us a little about yourself.

Jack Clabby: Well, I'm an attorney and I specialize in cyber security law. I also do work with corporations and individuals who are sued, traditional litigation work. I grew up in New Jersey. I worked for several years at the US attorney's office in New Jersey doing both national security work and cyber security work. A company would get breached or hacked and I would be there with the team of FBI agents or Homeland Security agents and we would respond to it. And sometimes we were able to catch the bad guys...

Mia Thomas: Right.

Jack Clabby: ...and other times we would do the very best we could but conclude that they were located abroad and no further action could be taken. About five years ago, I moved down to Florida, left government service, and started working at Carlton Fields. About half my practice now is working on cyber security matters and the other half is fiduciary duty litigation, corporate governance litigation. So, thanks a lot for having me here and looking forward to talking about what CPAs both internal and external can do to help protect both their own firms and the companies that they're working with.

Mia Thomas: Now, sometimes you use the phrase, "refeathering the pillow." Sounds nice and cushy, but what does that mean?

Jack Clabby: Yeah, so refeathering the pillow. I try to create terms that are easy to remember that stand for more complicated concepts. The idea of refeathering the pillow is, it comes out of a story I heard when I was a kid about rumors. Right? Telling rumors and gossiping is like going to the top of a

mountain with a down pillow and ripping it open and all the feathers will blow all over the world. Right?

Mia Thomas: Yeah.

Jack Clabby: And once the rumor or the gossip is out there, you really can't go and pull...

Mia Thomas: You can't contain them, right?

Jack Clabby: Yeah, that's right. And cyber security breaches are a lot like that, particularly for trusted advisors like CPAs, right? When the information gets out there, it is really hard to claw back those relationships and it really is hard to go and gather that data again and make it as if it didn't happen.

There's a lot you can do to come back from a breach, but the best thing to do is obviously to make sure it doesn't happen in the first place. And we approach this from two angles when we talk to CPAs. We think about what they can do to protect their clients, right, if they're either internal or external. But also, what they can do to protect their own firms.

Mia Thomas: You recently spoke at the FICPA mega-conference and you talked about cyber fraud and examples of the perpetrators of cyber fraud. Can you share with us some examples of who these people or organizations are?

Jack Clabby: Thank you for having me at the Florida mega-conference. And it was outstanding. Several hundred CPAs networking with each other, all in a great setting at the Disney Contemporary Resort. So, I'll tell you, I had a great time. And I had to tell my three children who are 10 and under that I was at Disney, but they weren't able to make it.

Mia Thomas: Oh, no. Well, next year. How's that?

Jack Clabby: That's right. We're going to, maybe we'll go through the slide deck with them, I told them.

So, there really is. There's internal and there's external fraud. And when we talk about fraud, right, we're talking about who are the bad actors who the CPAs have to look out for?

Let's start with external fraud because I think that's what most people are most familiar with. I mean, these are the hackers that you read about on the news. It's foreign entities in Iran and China or Africa who are trying to breach US companies because they either want to directly steal money from them or arrange a wire from a bank to be disrupted and sent to them as opposed to its true recipient, or

they're trying to get the data that the US entities have because they want to sell it either on the dark web or a buyer that they may have already set up.

Mia Thomas: And as you mentioned before, when you were working in your other role, when it's foreign, it's really hard to go after those foreigners. So, let's be proactive and keep those outsiders in. So, continue on.

Jack Clabby: That's exactly right. And so because these threats are non-US and because there are so many of them and the barrier to entry is so low to commit these email based or website based frauds, we have to put up a somewhat robust defense.

Internal threats are a different story. Right? Internal threats are familiar to any of the auditors who are listening to us now where you go out and you look for misuse of funds, or you might go out and look for expense items that are off. Right? Looking for cyber fraud is no different. You really have certain profiles of internal actors. We get a lot of calls from companies about disgruntled employees who are suspected of or did take data. And often they're taking the data to set up their own company or to sell it to a competitor or just because they're angry and they want to do something and they don't know, this may be the only thing they can do. And when that happens, you have a little bit more control. Right? You can get law enforcement more involved if it's an internal actor.

But, the timing for this is often when promotions are announced or when compensation is announced. People who feel they didn't get compensated enough or didn't get that promotion that they wanted may look for other ways to gain value out of the company. We've had examples where, you know, working with hospital groups where individuals went through a divorce and then they use the hospital system to look up the medical records of their ex-husband or ex-wife.

Mia Thomas: Oh, wow. Yeah?

Jack Clabby: And, we had examples where you work with a company and maybe the promotion didn't come and you have a head of sales or technology officer who's suddenly observed on the networks of the company at 1:00 in the morning, 2:00 in the morning, taking off gigabytes, terabytes of sensitive data that they really don't need to be accessing at 1:00 in the morning. And so what happens then is we'll get a call. One instance that I like to talk about because it involves an accountant who was a chief technology officer who was taking data out and actually when it was discovered by the information technology staff, the first thing that staffer did was went and told internal audit. And internal audit then told the general counsel and the CFO and we were brought in to help fix the situation. But, you have these internal threats that are observed by people in real time. They need to know how they can report it up through the system. Many of them think of internal audit first.

Mia Thomas: Well, what you just gave as an example, how did someone figure out that someone is getting that data?

Jack Clabby: So, I think two things have to happen right for that bad guy to get caught. Right? This is the internal threat who's taking data off the system. Very common in sales or retail organizations. The first is, the weird behavior on the network has to be found.

Mia Thomas: So someone's monitoring the time of day or activity.

Jack Clabby: That's right.

Mia Thomas: And so you should have someone in IT doing that.

Jack Clabby: That's right. It's IT. But then the IT person has to feel as if they are empowered or have someone in the organization who they can go to and report this. Right? Because if weird things happen and the weird stuff is, you know, it's often a high rank sales executive, right, who's angry about her compensation and is going and doing the bad stuff on the network. If the IT person doesn't feel as if, well look, you know. I'm an IT person and this is someone who makes a lot of money for the company. I'm not going to go report this to anyone because I'm going to get in trouble. So you need to have a culture where there's a strong internal audit or a strong general counsel's office where there can be communication.

Sometimes, right, it's the external auditor who may be the person who either discovers this or during the course of their assurance work, someone approaches them and says, "Hey, I don't know who to talk about this, but I observed something weird. Here's the thing that I observed. Can you help me?" And, of course, under the auditing standards, right, there are responses that have to happen for that. This has happened for us a few times in the college and university environment where the external auditor has caught, not because of any assurance work they did, but simply because of routine interviews they were doing, someone mentioned to them, "Hey, there was this odd thing that I noticed a couple weeks ago." And at that point it's escalated, goes up to the audit committee of the board of trustees and there's a communication to outside counsel to get involved.

So, you need to have the two pieces. You need to have some observing going on on the systems and then you need to have a reporting line set up so that the folks observing it feel that they can really listen to and have someone who can take action on the other end of it.

Mia Thomas: So would you call that a whistleblower policy or not that?

Jack Clabby: Yeah, no I think it can look a, you know, it can look like what we're familiar with from Sarbanes-Oxley. But it's really a cultural level. But some of it too is policies and procedures. Right? If

a CPA firm is writing its policies and procedures for incident response, right, a lot of times it'll say, and this is a maybe a 10 page document that says what to happen if you suspect a breach is going on. Often that first paragraph says when IT or information security discovers a potential compromise to the system this policy kicks in. What it should really say is, when anyone including - and then list a whole bunch of people - observe unusual activity on the system or suspect an incident, here are the steps they should take. Here's the number they should call. Here's the email they should send a message to. Because it really is the responsibility of everyone across the organization to be aware of and escalate it. Incident detection and escalation is something that many auditors are quite familiar with.

Mia Thomas: Right.

Jack Clabby: So this concept is not one that is foreign, but it is one that I think sometimes we forget. We think my system security is just the province of information technology. That's what we pay her for. I don't have to be vigilant. But really the incidents that I think we catch and we catch early enough are the ones where it was brought by someone who's not an IT or information security specialist.

Mia Thomas: So, we talked about detection. How can we be more proactive? You mentioned the incident response policy that can be drafted. What else would you suggest?

Jack Clabby: That's right. So, I think the account's role, the whole firm role that the accountant has is critical here. Right? Because if you think about an accountant who's internal at a retail organization. They have an opportunity to see how money's being spent across the organization. And then at the higher levels, you have the CFO, treasurer, and the reporting lines into those two positions. They are seeing the whole firm. So, when I'm designing a security program for a company, I want to make sure I have someone on that team who has the whole firm view. If it's just sales or if it's just collections or even if it's just information technology, I'm missing that whole firm view. I want someone who's involved in budgeting and I want someone who's involved in risk and assurance. And I think the accountant's role internal to an organization is to make sure that assets and resources are allocated correctly to the protection. It's not IT's responsibility to make sure IT has enough budget. Someone needs to be asking those questions. So, two things: I think budgeting is a huge part of it, and the accountant has a critical role in that; and two, I think it's the whole firm view of the accountant to say are we or are we not taking into account the entire risk?

And the third piece is having training programs within the firm - and this is true for both accounting firms and larger organizations of which our accountant listeners are a part. The training programs need to not just be for information technology staff. It needs to be for anyone who has access or potential access to sensitive information on the system. You have somebody in payroll, you have somebody who's involved in the tax preparation for that organization. They should be trained on what to look for, for odd system behavior and what to look for, for external threats to the system.

The preparation of payroll, particularly around W2 creation and 1099 creation is a point where a lot of foreign actors want to insert themselves in the systems. We've seen a number of W2 or payroll compromises that can be significant for an organization to recover from. When you think about refeathering the pillow, right, think about all the scattered feathers that go out when there's a W2 compromise at a large organization. And often that insertion point for the bad guy is in payroll.

Mia Thomas: Right. And we don't want to be reading about that in the newspaper.

Jack Clabby: No, no you don't.

Mia Thomas: Especially when it makes the front page of things like that happening.

Jack Clabby: And I think a lot of it, too, is just, you know, empowering individual employees to understand that if a senior executive reaches out via email and asks for sensitive information, the folks in payroll or the folks in the tax department don't have to respond to that. They're allowed to question that. Because the way a lot of these compromises work is the bad actor will either pretend as if they're the CEO masking an external email or they'll actually hack the system and send a real email from the CEO's email box over to payroll over to tax and ask for the data to be sent sort of on a rush basis often Friday at 3:00 or 4:00 o'clock. And the way to sort of fix that, right, is not with any particular system security. It's with going once or twice a year to the payroll people, HR, or the tax group and saying you're allowed to question if you get something that's weird from the C-suite. You're allowed to say, I don't want to send you all these W2s.

Mia Thomas: Right.

Jack Clabby: I don't know why you need to get a copy of the bank account and routing number for every person who works in the organization for the auto pay feature for our payroll. And having a culture where you can have that kind of control is critical. And I think the professionals who are in those organizations can self-govern. We had a, you sometimes hear stories of CEOs whose companies were compromised because it was their email that was spoofed...

Mia Thomas: Right.

Jack Clabby: ...or faked.

Mia Thomas: And I've seen that because it's easy. Look on Sunbiz or look on a website. You can figure out who the top players are and you can put their name in. But the email address, if you look at the email address, it's not their real email address. But their name is in there.

Jack Clabby: That's right. And, you know, the easy way to test that is have your mouse hover over what looks to be the CEO's email address or the CFO's email address and you'll see it's really not @your company. It's @gmail, but it's masked. In more sophisticated compromises, though, and we've seen a couple of these recently and they can be really bad. The bad guy has gotten into the system and is really sending a real email. And so yes you can try to protect the bad guy from getting into that system and there are technical ways to do that. But, the cultural way, the way that's in the control of everyone who's listening is have a culture at your organization where professionals who touch sensitive data can question requests that come on.

Mia Thomas: Realize that this isn't a true request.

Jack Clabby: If you work at an organization where or you observe it as an outside auditor, if the CEO walks past the employee in the hallway is the employee told don't make eye contact, don't say hello? You'd be surprised how many organizations have that kind of a culture. I love to find out from an external auditor if they ever ask that question. Are allowed to make eye contact with the CEO? Because my guess is when you get an answer that's no, something is going on in that company that...

Mia Thomas: Not good.

Jack Clabby: ... is either something's happened or there's a risk.

Mia Thomas: Yeah. We'll put that in a survey. How's that?

Jack Clabby: I'd love that. I wonder.

Mia Thomas: You should do that next time you speak.

Jack Clabby: I love it.

Mia Thomas: Have that in a survey. Well, Jack, we really appreciate you being with us today and sharing your insights on refeathering the pillow on cleaning up cyber fraud. This is definitely something that everyone should be considering for their organization if they haven't already. Jack, tell our listeners how they can get in touch with you.

Jack Clabby: Well, thank you, Mia. So, I have an email address and I'll share it with you. It's jclabby, C-L-A-B-B-Y, @carltonfields.com. But because of what I've just told you about being skeptical about email, call me. Alright. My number is 813-229-4229. Or check me out on LinkedIn.

Mia Thomas: And I appreciate you telling about this incident response policy that I don't think many CPA firms or companies have. That's definitely a must to-do list for any company to have. We

appreciate you. In FICPA we do have additional resources, continuing education opportunities, or to have someone like Jack come to your office and help you prevent or correct cyber fraud. You can visit us at www.ficpa.org or call our office at 850-224-2727 to get more information. Until next time, keep smiling.

Presented By

John E. Clabby

Related Practices

Cybersecurity and Privacy
Technology

Related Industries

Technology