Training Law Students for Cybersecurity Practice

Stephen Black, Texas Tech University School of Law

PROFESSOR BLACK: We’re going to go ahead and get started. My name is Steve Black, and I am just happy to be here. I realize that I may be last right before we’re going to go eat and do things, so I’ll try and be entertaining as we do that, and like the other presenters, if you want to interrupt me, it’s not going to bother me at all. So, we’re going to talk about cybersecurity practice, which doesn’t sound daunting at all. And I frequently get asked questions about what is cyber security practice? And what are we doing? Will that work? It will?

I don’t even know if I like this slide at all. But I get asked for this slide, what is a cyber lawyer? And so, I put up a whole bunch of interesting things—that’s somebody who’s working from a computer, isn’t it? Mr. Robot, there in the or Ms. Robot there in the middle, I have no idea about gender or dealing with privacy, privacy policies. You know. What? What is it that we do? Frequently I get asked this question—what’s the lawyer doing in the room? I go to cyber conferences. I do all types of things. And so, here’s my answer with my school’s ask.

You know, what if we had a bunch of international criminal gangs taking in tangible assets? I was trying to think of all the legal things that I usually tell people, you know, and the resulting mess implicates notions of privacy and agency and property. And just not real property, but tangible and intangible property, including data, whatever that is, tort liability and international relations. Would that be a legal issue or rephrased? If there’s a problem in your organization and we’re in the middle of a breach, are you going to call legal? And the answer usually is, yes.

In that case, I think we probably need to think about training lawyers to be the person who’s going to receive that phone call. I just picked a couple of headlines that I found very quickly off of Google. First, in the first half of this year, we had a 49% increase over last year’s number of publicized attacks. That was a one-year year-to-year increase of 49%. And I asked people the question, do you think that the criminals are giving up? Are they getting tired of this whole thing?
Second, the global cybersecurity market set to exceed 7.8 billion dollars. Is that a lot of money? At lunch we were talking about how I go to cyber conferences. That’s why I get all the questions about what’s the lawyer doing here, and I judge the success of the industry by the amount of swag that they throw at me: T-shirts and mugs, and a lot of baseball hats and at some of the conferences I get glowing swords, and at this last one I won an Apple home product that I think is worth $150. And that’s a tax issue that I’m going to have to resolve later, whether I need to report that or not.

So if we’re going to train lawyers to do that, there are some foundational doctrinal classes we should offer. I started out offering two, and then I went to three, and I think I’m up to four. Here’s what I think some basic classes in the area would be: Number one, privacy. And that’s going to include the First and the Fourth and the Fifth amendments, torts and consumer protection, and maybe an intro to data protection as well.

Number two, data regulation—including the foundational question of what is data in terms of its legal aspects. I’ll just give you a hint of what I’m thinking about it. If we hadn’t had any legislatures intervene in this area, it may have been okay to say, data is kind of informational, and I don’t know how we classify it. But as soon as we start endowing it with rights, or, more specifically, start endowing people with rights with respect to their information and the other people who are collecting it. We tell our first-year property students that property is a bundle of sticks, and the sticks are rights. And so, at some point, if I have a whole bunch of rights with respect to my information, haven’t I made it into property? Nobody likes it when I ask that question, so I’ll go home at that point.

Number three, cybercrimes, and that includes a whole litany of property and access crimes, including some digital analogies to trespass, the computer fraud and abuse act, the wiretap act, sentencing, and jurisdiction. There are a whole bunch of fun things, if you like to teach criminal law. Sometimes they’re included in white collar, but you know these are more specific to just computer crimes.
And then number four, the latest one that I have been thinking about, is an internet or cyber law course. And sometimes this is the first course that we start thinking about, which can include Internet contracts and copyright and trademark and defamation, spam and social media issues, and there are a whole bunch of other things that probably should go in there as well.

But what do these foundational doctrinal classes equip students to do? I always start with this all right: So, I’ve got some doctrine behind me under my belt, and I’m ready to do this. And everyone’s favorite rule is this competence rule? Not really that we should be competent. We all agree on that. It’s this comment that popped up a few years ago, the benefits and risks associated with relevant technology which some of us in the tech space use to bludgeon our colleagues in faculty meetings saying, Yeah, we need more tech classes. In any event, here’s the question. Once I have the doctrinal classes, am I ready to take that phone call of, “Hey, we’ve just been breached. What do we do now?” So, what is the attorney’s response? My colleague, who is a Chief Information Security Officer, put this “incomplete” list together, and it’s way too small to read. And I’m just going to tell you what it is. It’s a whole bunch of different areas of cybersecurity that are interesting, but it’s going to deal with things like network topologies and cryptography and career development and thread intelligence, and a whole bunch of other things that most of us look at and say, “I have no idea what we’re talking about.”

To illustrate, let’s talk about the Las Vegas MGM Grand. On September 11, 2023, the MGM reported that, “Hey, we may have a problem. We’re going to shut everything down. And by shut everything down, that means that all the slots and all the rooms and everything else that we do are going to go dark.” They still had guests there that couldn’t get into their rooms or out of their rooms, for that matter. By all estimations MGM Worldwide is making about 8.4 million dollars a day. That was the number I was given, and they were closed for a good 8 days. Probably about two hours
ago I got an email that said the total number is about 100 million dollars of loss that they suffered.\(^1\) Well, here’s what happened, according to my sources:

There’s some sort of breach. Two different groups have taken responsibility for it, and we can’t really know if either of them is telling us the truth. But basically, what happened is a hacking group called the help desk, and they said, “We have an account. We need to change the password. Can you please help us?” The guy at the help desk said of course and changed the password. At that point, the group locked everyone out of the Okta server, which is basically MGM’s centralized authentication and authorization server. Since everything is digital, including your room key and slots and credit cards and everything, the hacking group locked everyone out. Which means MGM went dark—can’t even get into the front door.

So, the question is if that type of breach is coming to general counsel’s office, does general counsel need to know something about what that server is and what it does? And if so, then my colleague’s “incomplete” list becomes interesting. Not that I need to know everything on it, but if I don’t understand what’s going on, then I’m going to have a hard time assisting in the remediation process.

Which brings us to our next question. So, I’ve got four basic doctrinal courses and a smattering of tech knowledge. Is that all I need to know? All right. Now, we’re ready to have a lot of fun. So, I like to make lists. So why don’t we start with talking about what lawyers can do before a breach, and then during a breach, and then, after a breach, and for my simple mind that three step process is going to be really good for us.

So, before a breach here are some things that lawyers can do in the cybersecurity. Number one is inventory. To help our organizations, we can start by mapping why criminals do what they do or the motivations behind what they do. The thinking being, what do we have that a criminal would

---

want? Absolutely fascinating question. I will tell you that I’ve asked that question of a lot of organizations, and the answers I get are variations of “I don’t really know what we do, but we’re making a lot of money doing it to.” To which I respond, “Well, let me start to make a list of the things that we think that somebody could attack us for and want to take.”

So, I can help organization’s inventory. I can help organizations identify and protect, by asking “What do clients identify that they think is valuable?” Is it data? Is it intellectual property? Is it reputation? Reputation is a fascinating thing. “I didn’t want to hack you to make money. I just wanted to destroy you. I hate you completely, and I want to bring you down.” Is that a hacktivist? It absolutely is. And do I need to think about how I would help an organization protect themselves against that assessments?

Are we any good at defense? And I say this because my football teams let me down last weekend, all of them. It was really sad, and some of our organizations also do the same thing. We think we’re really good until somebody who is smarter than we are comes and takes over our organization or shuts down the casino floor. That’s fun. Do we do assessments of where we think problems may arise?

Imagine an overturned school bus. This is not me suggesting that we should overturn a school bus, but it makes a great mental image, and the realism is helpful. Part of what we can do is help. Law students understand that when we’re confronted with these things, the school bus may be turned on its side. And the question is “All right, so, how am I going to help my team get that over? And if there are legal issues such as were there people inside? Were there people outside?” What are we doing with these types of issues?

Now, let’s talk about how we can do some skills training before the breach, and talk about vendors and third-party practice. There are very, very few businesses that do not belong to a supply chain of some type, which means that they’re using vendors to do part of the work. They’re using third parties to come into their organization. And as lawyers do, we think about how I can help protect in terms of vendor contracts? Do I think about how
I can help protect by exerting influence on others that interact with my organization to help them adopt best practices that my organization is trying to adopt themselves? So, this third-party practice of who else in my space do I need to consider and think about is something that lawyers can do as well.

So transactional skills before the breach can include inventory skills, assessment skills, incident, and response planning. That is, considering if were going to turn over the school bus, what would happen next? And it’s a fascinating area for lawyers to come in and feels really natural to us. Because I don’t know about you, but nobody invites me to dinner parties, because in my mind I’m always thinking, what’s the worst that can happen in that potato salad right? Has that been refrigerated or we all going to get food poisoning? That’s the way we think. And I’m sorry, but we’ve all been right completely ruined, by the way that we think about things, but it’s a perfect skills exercise for incident response planning.

So, if you have a client that happens to be a casino, and somebody calls up and asks to have the password changes, and the person behind the help desk changes those . . . what would you do next? Who would you call? How would you call? You know you ought to think about how you would call, because in this scenario the criminals who had breached the system had gotten so far into the system that they had also breached the Zoom passwords. So, when the casino called in the world-expert-incident-response-threat-hunter-white-hat-hacker people, the criminals have access to the recording of the Zoom Meeting where the white-hat hackers were talking about how to get the casino’s network back. And I can just imagine in the criminal den, right—that’s the only way I can think of it—that they were laughing their heads off, thinking we’ve owned you so completely.

So, the new thinking is that you should have secondary communication channels. Well, that doesn’t come up unless you’re really paranoid—like a lawyer—to say “What would happen if the hackers had breached our communication system, too? Because I wouldn’t want to tell them what we’re going to do next. Otherwise, that breach is going to continue for a long period of time.”
Incident response planning is an excellent exercise. I was teaching a class at the University of Houston, and I asked my students to put together an incident response plan. I gave them different clients. One of them represented the organizer of a music festival, and another one organized it for a school, and whatever. And I said prepare an incident response scenario that you would use for training and then give me some slides. And I was blown away by what they came up with in terms of “Here’s what you need to think about.” One of them actually made an interactive. “Choose your own adventure,” they said, “All right. Here’s what’s going to happen in the breach and choose slide A or slide B.” And I thought, “Okay, I’m game. Give me some popcorn. I’ll choose Slide B.” And they said, “Great. Here’s what’s going to happen next.” A very low-tech, very exciting presentation that they came up with. That made us start to think, “Okay, this is what we need to do to prepare for? Not if, but when we get breached?” Students can adapt to this very easily.

All right, and vendors. What skills do we need to know? Let’s consider DLA Piper in Baltimore. One of my friends, who is absolutely brilliant in terms of crisis communications, says you should be very careful who you hand the microphone to. When DLA Piper was breached some enterprising soul thought, well, let’s get a whiteboard, and we’ll put it in the lobby for crisis communications. The whiteboard read: “ATTENTION DLA EMPLOYEES- All network services are down, DO NOT turn on your computers! Please remove all laptops from docking stations & keep turned off *No exceptions*” Images of this whiteboard are widely available on google images.

Now, can we train lawyers to be involved in the process of crisis communications? Yes. Can I train my vendors? Have the lawyers train the team that if we have a breach there are communications and protocols, which means: “Don’t talk to anyone from the press.” Why? Because as soon as it goes to the press, I’m going to be seeing it in a later lawsuit. The question goes back to something you talked about when you’re training the students, and they’re thinking about incidents. You can do it in the format of a tabletop exercise or in terms of “I’d like us to draft an incident response plan and here are five things that I’d like us to think about. Or here are three things I’d like
us to think about, and I’d like you to come up with two others that aren’t on my list. Can you do that?” And then can we run through that in a scenario and see if we actually covered everything or something else is going to happen in an emergency. All bets are off, and it’s great if legal tells the organization, “We’re going to practice this. Yeah, we’re going to turn the bus over and then see what happens. And then we’re gonna learn from our mistakes. And I’m gonna go back and here’s incident response plan version two.”

Another example comes from Broward County Public Schools when they were hacked. The criminals in that case were able to use public records data to find out what their operating budget is. Then they figured out that they could just ask for a percentage of that as ransom. The school had to come back and say, “We don’t have that kind of budget.” But watching this transcript unfold, honestly, it gives me worse chills than if we were negotiating for the return of a kidnap victim, because just the brazenness and the evilness of the hackers here, in terms of this is what we’re going to do, and we don’t care about the fallout. This is going to be the context that we train individuals how to negotiate. While I’ll be presenting some skills today, I’m going to tell you that you don’t need to have a complete cybersecurity program to implement. If I taught a negotiations course, I may want to pull in something like this. Not that I don’t know if I know anyone that’s brazen enough to be on the other end of the text chat that would just say, “We don’t care. We’re gonna destroy all your data. And all those kids are going to be—you know—without education.”

It’s important to train individuals to be involved in the ransomware negotiation process for those of you that are now thinking about it. The ransomware process is also important because it involves a whole bunch of legal issues. Number one, do you pay it? Is it legal? Is it ethical? Is it advisable? These are criminals we’re dealing with. Sometimes the technologies they use are not perfect. So even though you’ve just paid them thirty million dollars, you may not get the data back and nothing stops them from saying, “You just paid us thirty million dollars. We want another fifteen.” So having students think through that process is a wonderful exercise, if they are
thinking about going in-house or representing individuals that have been breached.

So, I’ve got Rand somewhere. Yes, I may get a comment. What percentage of these just turn out for the transmit. It’s pretty high. It is fairly high. I don’t have numbers for that right now, but we’re 49% higher than last year. It was just an increase of every reported ransomware incident from the first quarter of 2022, and we were 50% higher than that in the first quarter of this year.

In addition, in June of this year—it’s October so June of this year—the White House did an about-face. Originally, they had said, “We’re not going to get involved in the question of whether it’s legal or illegal.” They, in the process of bringing over several of our trading partners, made an announcement that they’re now considering making the payment of ransomware illegal. Several States have already done that. So, it’s a State-by-State determination, but also from a federal point of view, they’re considering making the payment of ransomware illegal. That’s not going to stop the extortion. That may just stop the payment of a ransom. That’s a legal issue. So, bringing the concept into the mix of “what are you going to do as you’re responding to these types of things” I find to be all kinds of interesting. No one likes me. And this, number one—I have to make this clear—I highly respect my colleagues in law enforcement. I love them. They are very, very talented, but it’s a legal question of whether I am going to involve law enforcement in my organization if we are breached.

Here are some of the issues that that I think about: number one, is law Enforcement’s team better than my team? I don’t bring in people who are not as good as the team I already have in place. Number two, and I hesitate to bring this up, but what will they see? Everyone says, “I don’t have that in my organization.” Okay? Good. Unless they are going to see something in your organization. And then I’ve got a question, have I waived attorney-client privilege because I was the one who invited law enforcement to come in and help us with our breach? Number three—I guess—can I limit the scope of their investigation? “I would like you to help me with my breach, but if you see anything in this closet, it’s off limits.”
Number four, when will I get my drives back? Because law enforcement is going to take a copy of or seize all the computers to do further forensic analysis on them. Number five, because we all love contracts, have I breached any third-party agreements that I have? In other words, have I now disclosed information that somebody else told me that I wasn’t allowed to disclose, and I disclosed it to—the horror of horrors—the government!

Those are all fascinating issues happening very quickly, because if I’m in the middle of a breach I may need help. I may need to bring people in for translation. Maybe I have absolutely no idea what we’ve got going on, but in an organization I may have IT, people who understand what’s going on in the first bubble, and then I may have the C-suite, or the business people who understand what’s going on, in the second bubble. I can tell you frequently that they are not speaking the same language. We know that because frequently we [the lawyers] are using a third bubble, and nobody understands our speech either.

We can train lawyers to translate between the two groups by saying, “Listen, I understand that we’re worried about money, but you need to know what this other group is worried about and here’s what’s going on with that.” So transactional skills during a breach include communications, ransomware, transactions dealing with law enforcement, and translating between the C-suite and the tech team. I can create skills exercises, even if I don’t have a full cybersecurity program at my law school dealing with any of these, or even by mixing and matching some of these skill exercises. It’s very useful for students who, at some point in their careers, may say, “Huh! Now here is something that is cybersecurity in nature.”

I was teaching a class dealing with in-house counsel, and I skipped having a cyberware class. I couldn’t find another attorney to teach it, and I felt like I just didn’t know enough about the technology itself to handle a tabletop exercise. I knew I wanted to do a tabletop exercise, because that’s where you actually have something arise at your company. So, I guess I’m wondering how much do you have to know about the technology to teach such an exercise? It’s a great question.
And the answer is you can design it to teach as much as you want to know. Frequently in organizations the tech team will go through a tabletop exercise, and it’s completely different than what the business team will do, or even what the legal team will do. We design it in terms of a network, and everyone is sitting with a laptop. We tell them, “Here is what we’re going to do. Here is what is happening, and here are the messages that we’re getting. What do you do next?” It involves typing commands. That’s not usually what the legal team does. So, we can design those exercises around simulated experiences.

I won’t start a clock necessarily, but I can if I want to. It adds pressure, and people make mistakes and do all kinds of things under time pressure. I can simulate that because I’ve gone in and said, “I understand how this one area of the cyber domain works.” So I’ve designed an exercise around that to help simulate when somebody calls you and says, “I think we have a problem.”

I’ve had an experience where one of the hypothetical workers in an organization was traveling to a conference and lost their laptop. So, it’s only a lost laptop. Do I need to know a lot of other things? No, because now I’m looking at just physical loss. I can understand what’s going on there. I can understand what’s going on in terms of passwords and other types of things on there, and we can tabletop that in terms of what do you do first; such as, who’s the first person that you call? Is there a process that we’re going to go through? Usually I pair that with an incident response plan, either one that I’ve done or one that I’ve had ChatGPT do. It’s got some flaws, because I want the students to see the flaws in the plan so that they can take the next step by determining how to fix it.

We’ll then reset the hypothetical, and I’ll have them tell me what they’re going to do at every step of the new problem. It’s a very illuminating process, even for non-hypothetical clients, because you can take that into a business and say, “Here’s what we’re going to do. Your incident response plan says you’re going to do this, this, and this. I’ve designed a problem and now we’re going to test that. You’re going to tell me how you’re going to respond.” I’m also having the legal team and the business team watch as the employees go through this. Then we’re going to ask whether that was the
best response. It’s a great question. The answer is I can do it. And this answer can involve all kinds of technology or the answer can be fairly technologically agnostic and still get the same results. I have had to provide such answers.

Now, when I consult with other people, I take the role of the lawyers to say, “All right, what might we do about a data breach? Do we know our deadlines and what’s in our customer contract?” I think when the legal person comes in with those kinds of questions, we want to make sure somebody has thought about it. It’s nice to know, because our role as attorneys is to highlight the big picture things a company’s employees have to talk about, such as who’s going to do what and what they’re going to tell the Board. What if the company’s national cross-border data is involved? We should know something about the technology. Many of these companies are super small firms or companies that don’t have a privacy lawyer. That is why I think it’s so important to have everyone that is involved with the company to at least have some training.

Here’s a simple hypothetical. You think your company has been breached and you’re worried about data being removed from your network. One of your IT staff comes to you and wants to know who did this and how, so they can prevent it from happening again. If you turn off the computer, you may lose all that information. It may have been the type of hack that may be in the memory. Nothing was saved on permanent or semi-permanent storage. It was all in RAM. If you turn the computer off it goes away and you’ve destroyed the evidence.

Should you worry about saving the evidence or the data? Which of those is the more valuable proposition? This is an extremely fascinating hypothetical to run through with a group, and you’re going to find different parts of the organization will give you different answers. Have a group discussion about what the students think should happen and what they intend to put in their plan. You can teach students to do that so that they’re asking the right questions. After the breach, the house does not seem quite stable. After the breach, what’s going to happen? This is a lawyer’s dream. Something bad has happened, and now we get called in. And what are our priorities going to be?
Number one: insurance, lawsuits, and risks. Cyber insurance is everyone’s favorite topic. No one likes to talk about it. Let me give you a couple of thoughts about what we’re talking about in terms of claim denial, which also speaks to what occurs before the breach. If I am counsel for the company, we’ve spoken with our insurer and underwriter about what our policy should look like. Here’s some reasons for claim denials:

- **Wars or acts of God.** If it was a nation-state who attacked me, does the insurer get to say they don’t have to pay for that?

- **Failure to maintain standards.** In other words, this was the company’s fault, because you didn’t update your systems, allowed someone at your help desk give the password out, or it was social engineering.

I remember a particularly instructive video on social engineering where the social engineer is sitting with the reporter saying, “Give me fifteen minutes, and I can get your password for your phone account.” And the reporter said, “no, you can’t.” Then the social engineer opens her laptop, starts playing a recorded music background of a crying baby, calls the phone company and says, “I’m sorry the baby won’t go down right now, and my husband told me I had to pay the bill.” Now, watching this video, I’m feeling sorry for her. Except that I’m looking at her knowing that she’s the evil social engineer. Social engineering and human error are usually an insurance exclusion. Ransomware is another fascinating one. If you pay the ransom, the insurer won’t. Well, that’s fascinating for the legal team to say, “We may want that option in the future.” Are we looking at how our insurance is dealing with the cyber problem?

This is the scary part where legal theory then becomes real, and we really didn’t want it to be real. This is the theory of cyber accumulation risk. Again, there are very few businesses that operate in a vacuum and are not part of a supply chain. If I get breached and that breach filters down to other members of my supply chain or other members of my industry, are they going to look at me and say, “We can sue you, because you were the weak link in the chain.” If I am legal in a very strong organization, I’m looking out over everyone else in my industry group, saying, “I don’t know about you
over there, because I don’t think you’re as cyber-aware as we are. Do we want to do business with you?”

Incidentally, another insurance issue is that if I get breached because someone else in my organization or my industry group got breached, will they pay right now? The insurance models don’t cover that, but it’s something that we, as legal risk managers, should start to think about.

The third area of risk and liability occurs where the company just hired a really smart person to run our cyber organization. That’s our CISO, our Chief Information Security Officer. Now the CISOs are asking, “Well, wait a minute . . . Am I gonna get fired if there is a breach at your organization?” Anyone want to guess what the average tenure of a Chief Information Security Officer is today? It’s less than 24, and more than 18 months, is the right answer. How many of us would take a job where there’s a really, really, really high chance that you’re going to get fired in 18 months? Most of these terminations are due to some sort of breach, although sometimes it is due to poaching. Regardless it’s a very, very short tenure.

There’s a high rate of burnout among that group as well. Let’s think about how you don’t sleep day or night, because nighttime is the most likely time for a breach. The most likely day for a breach is going to be September 11th. That one is fascinating. The most likely time of the week for a breach is going to be the weekend. If there’s a holiday, you probably should have somebody on call, because criminals watch the calendar, too, and figure that nobody’s going to be in the building. It’s a good time for them to do what they’re going to do.

Which brings us to talk about trust. Are lawyers involved in building trust at all? Or is that kind of a marketing department job? What kind of trust are we looking at? Are we looking at customer trust? Are we looking at supply chain trust? Are we looking at investor trust? Earlier, I mentioned failure as a learning tool and whether you fire your CISO just because you got breached. It’s horribly expensive to go through that process of cleaning house and finding somebody new who’s going to make sure this never happens again. You’re working with them as well because that involves HR
and Legal. Do I keep people around and let them know that we’re going to work on these processes over and over and over?

And what about cyber-due-diligence? What to look for when buying a used car? Why is this after the breach? Your company’s been breached. Great! The water is fine, everybody jump in. Because it’s not an if, it’s a when you’re going to get breached, right. If I am in the M&A space, we do legal due diligence, and we do financial due diligence. I may do contractual due diligence. I may even look at the people involved in the organization. The question is, who’s doing cyber-due-diligence?

You may remember a number of years ago that Marriott purchased Starwood hotels. Marriott said this would be a great marriage. But somebody forgot to ask if Starwood had been breached and was continuing to be breached. The criminals were still in the network. When you marry two networks, what can happen? We just invited all the criminals in, and then Marriott gets to pay hundreds of millions of dollars in fines all around the world. You may remember also that Yahoo was interested in being acquired by Verizon. Someone at Yahoo didn’t think that cyber security was a material disclosure until about two weeks before closing. Is that a good time to find out about those things? Okay, do lawyers do due diligence? Absolutely. Question is, who’s doing cyber-due-diligence? Ask VC firms and investment banks, “Who’s doing the cyber-due-diligence for you?” I’ll tell you what the answers are, and they’re not pretty answers.

So instead, can we train lawyers to do cyber-due-diligence? Sure. Is it a fun practice? Sure. Because what are you doing? Number one, I’m teaching students about what is due diligence. What is its purpose? Number two, I’m teaching them about how it’s done. Number three, I’m teaching them what happens when I don’t get the answers that I want, either because the target doesn’t want to tell me the answer or the target doesn’t know the answer. A number of years ago I was asked to teach a series of seminars on this topic. In the first seminar, I had to teach everybody about due diligence, and then they invited me back and said, “Let’s ramp it up.” And I said, “Great.” I went around to a whole bunch of vendors, and I said, “Give me your tools and
let’s go ahead and do a hands-on thing.” So, here’s what I did. I used a company that does a real time map of data flows.

So, some of the questions you ask are, “What computers do you have in the building? IP addresses? What am I looking at in terms of scope? What does your network look like?” And I’ll get an answer, and I may or may not know what that answer looks like. I sometimes need permission from the target to install a tool on their network. In real time I can see what machines are on the network and how they’re communicating with each other. If I have a database, I can see who’s making requests and where the data is going, in both directions. That’s absolutely fascinating. If the target has given me a list of IP addresses, I’ve got this tool on their network, and somebody at some point said, up there in the right-hand corner, “What’s that IP address?” The target’s Chief Information Officer said, “I don’t know. I don’t recognize that number.” At the time they were pulling lots of information out of the main client database, at which point we stopped the installation and said, “Okay, this is no longer an installation exercise. You need to call your insurer. You’re in the middle of an active breach.”

That doesn’t usually happen, but it’s fun to see. Awesome. Sorry, that’s perverse, right? Not fun to see, but in terms of a due diligence process, it’s great to see when they say, “Listen, we’ve only got five machines in the building and my tool shows ten from a due diligence point of view.” What do I do with that? Well, that’s a great thing to have students consider—how do you go make a decision based on the tools that you’re giving.

I also have a set of tools that works like this: we have a list of known attacks, we catalog all the attacks in the world that have happened, and we put them in a big list. So, what if I put two apps on your network? One is the hypothetical bad guy, and one is your machine. Then I launch all of those attacks against your network. Not really. But I’m doing it hypothetically launch them to see which of those might get through. Then I’ll have a list of which hypothetical targets or attacks could get through. Then from that list, I’ll launch a whole other set of attacks and see how far those attacks could get and I do it until I see how far an attacker could get in your system based on how your system is configured for due diligence purposes. Would you like
to have a list of what may happen? Not that it has, but what may happen in terms of what price we should pay for computer assets? Those both need permissions to get into the system. The last one doesn’t. It’s a tool called Maltego. I should warn everybody here—they’re happy to give out free academic accounts. Your life will never be the same if you do that.

For those of us that are academics and have access to Lexis, we know that public record searches are sometimes available on our versions. Think of this as public record searches on steroids, because you can install open-source intelligence databases like you do apps on your phone. Then you can take those and combine them together. For example, if I wanted to do a person of interest research project on all of the owners of a business that I was going to acquire to see. I don’t know. What can I see? What kind of real estate do they own? Where do they do their banking? Whether they’ve had any social media accounts now or in the past and anything they’ve said on those accounts? I can do that, and I can pull it all up and get actionable intelligence on it. Can I see if any of them have ever done business with anyone who’s on a sanctions list? Yes, I can. Would that be important. Yes. Not that I necessarily care that they’ve done. Oh, wait a minute, yes, I do, because if that gets out in the public then this merger is maybe a bad idea. I was preparing to do a presentation like this, and I was using this tool, and I thought, well, it’s not going to hurt. I will just do a quick search on some random Dallas law firm that I picked somewhat at random. With the engineer that I was working with, we ran one search, and he said, “Oh, you don’t get to use this at all.” I had to redact all but part of what I found. It’s not illegal for me to look at sources found on the dark web and see that your passwords are out there. It probably is illegal for me to use those passwords, and it’s probably really, really inadvisable for me to put them up on a screen.

Here’s what I had from several of the staff at the law firm. I had passwords to not only their email accounts, but several of their social media accounts, and they were in plain text. I had residential addresses of several of the partners. That’s probably not information I wanted to share on a big screen either. I found out that one of the partners was moonlighting because I was able to find the website of the law firm that they were moonlighting for, and the password for that. I had all that up on the screen, and it was one
search that I had run against one of the databases. This is why I said they’ll give you the account and be happy because they’re looking to have more people trained on this because the information is out there. Training law students how to gain information is legal research. If anyone’s interested, I’d be happy to put you in touch with them. I’m just going let you know, some sleepless nights may ensue.

The third part of this is how to prepare a due diligence report. How do I draft the information that I found to say we really shouldn’t do this deal, or we should do this deal, but we should ask them for a 450 million dollars concession on the price? Those are absolutely fascinating things to train law students to do.

We’re not securities lawyers, alright. In July of this year, the SEC—what is the SEC doing in this area?—adopted rules requiring registrants to disclose “material cybersecurity incidents,” and to disclose every year material information regarding their cybersecurity, risk management, strategy and governance period. Question – who makes those determinations? How fast do we have to make those determinations? Having made those determinations, who do I tell? What do I tell them?

So, we’ve just been breached. Great. We have a very, very short time window to make a determination as to whether that breach is a material information item for our investors. We know what that standard is, or we think we know what that standard is. I’m still questioning it myself. Who in my organization should be making that determination. Should that be IT? Should that be the C-suite? Should it be legal? Should it be a bunch of us that get together if I find that there has been a material breach, and it wasn’t my fault, but it was someone else in my industry? Do I tell them? Do I keep my mouth shut? If I make a material breach report to the SEC, is it public? Yes. Have I just told other hackers how to hack us in the future? All these are fun questions that are waiting resolution.

If we train our students how to do this, I’m going to guarantee you that they will not be worried about jobs because there are a lot of these going on out there. And these topics can take up a full semester. The data regulation
course that I taught at Houston was a full semester. The four courses that I mentioned at the beginning of the presentation, each of those could be a full semester, or we could compact them down. The skills courses could be made into a full semester. The truth is, I’ve had a lot of people, both students and graduates—graduates who’ve been out for a long time—ask, “where do we get training in this area?” I’m letting everybody know that we can, “We can provide that training.” Could we make an entire master’s program out of it? We probably could if anyone is interested in doing that. Can I throw these exercises in and just get students to start thinking about it as a practice area? Yes.

What about transactional skills after the breach? That can include cyber-due-diligence. Can I train people how to do that? Can that train lawyers into teaching and training their organization to adopt failure as a learning tool? Can I make our defense better? You can be guaranteed that the criminals are using their failures to learn how to get into systems easier, quicker, and not be detected. Can I teach a whole skills course on SEC disclosures? I absolutely can. The general applicability date is December 18th of this year. What’s today? Yeah, it’s coming up. A lot of organizations are saying, “We’re going to get ahead of it. We’re going to try and do it.” Then the question is, what is material and what do I need to disclose? How do I hide the specifics of the breach so that I am not subsequently allowing myself to be attacked by everyone out there. Who’s a copycat? That’s an absolutely fascinating thing, both for in-house counsel and for external counsel. How do we go through these types of things?

Do I see that as a niche area that I could start a practice in today? Sure, if anybody wants to quit their day jobs and do that. We would have more work than we knew what to do with. We could also train our students to do that and cheer them on. Which is my solution to the problem.

Finally, is this job any fun at all? I’m going to tell you I’m enjoying it a whole lot. I know a lot of individuals who are saying, “Goodness! The criminals are winning right now, and my prophecy about what’s happening here is that the criminal activity is not going to decrease.” This area of practice—the disclosures, the pre-breach, the during the breach, and the after
the breach, the privacy practice—all these types of areas are going to combine to be a large area of practice for a lot of our graduates, our alumni and others. The more that we can say, “Here’s what we’re going to think about in terms of what skills can we give you so that you can respond to this, and that you can jump into practice and be ready when that dreaded phone call comes—hey—I think there’s something wrong with the network.” What do we do now is a wonderful addition and wonderful value that we can give to our students.

Do I have anything else? Not really, unless there are questions that we haven’t talked about. Privacy law? Everywhere I’ve worked, privacy and cybersecurity are completely separate lawyers. Does it need to be that way? Or do you see a lot of people having both cybersecurity and privacy? Does it need to be that way? No. I think as we look at it holistically to say, “What is it that we’re protecting?” I think part of it is that we are protecting the trust given to us by our customers who have given us their private information. We’re protecting the members of our industry who’ve given us their data to deal with and hold on to. I think it all goes together. My understanding of those that are engaged in privacy practice right now is that they don’t see that we should also be involved in incident response. Although, incident response is going to be responding to the value-added proposition. All that we can say is, “Let’s look at it in terms of is my board even ready to do this? And can I help with educating the board so that they know who’s going to be in charge if something unforeseen happens?” Alright, friends. We’re done for the day.