Lowenstein Sandler's Cybersecurity Awareness Series

Session 15 – Cybersecurity Awareness Month 2025: Legal Risks, Data 360, and Practical Strategies

By Amy S. Mushahwar and Ken Fishkn

OCTOBER 2025

Ken Fishkin: Hello, I'm Ken Fishkin, head of cybersecurity for Lowenstein Sandler, and welcome to another episode of the Cybersecurity Awareness Video Series. To kick off Cybersecurity Awareness Month, I have with me today, Amy Mushahwar, who is the practice chair of the Data Privacy, Security, Safety & Risk Management practice. Amy, could you tell a little bit about your practice?

Amy S. Mushahwar: Thank you so much for that, Ken. What we're trying to do is interject that there is an awful lot of content moderation and safety work, work that we're doing in bullying and trafficking, in the protection of vulnerable populations, that doesn't necessarily fit in the privacy or cybersecurity silos. And one thing that's also very innovative about our practice group that we debuted in September—and we're going to continue to tout for October because it is Cybersecurity Awareness Month—is that we are adding a new approach to something I've been doing for something for my entire career. Our approach is called **Data360**.

We are data lawyers, and we follow the risk in whatever silo or vertical that happens to be. So as I am data mapping your enterprise, for example, for privacy and cybersecurity basis, if I find other content management where maybe we might need to bring in an FDA lawyer for a mobile health or wellness perspective, or we notice that there might be issues if you're a financial institution with the automation of your data and perhaps fair lending, it is our job in the **Data360** group to have the hub and spoke to every major practice group in our firm and bring in the resources to bear on your multi-issue questions with data. We follow the trail and make sure that you have the expertise when you need it as we're doing the work for you. We're problem solvers by nature.

Ken Fishkin: I've been reading on the news a lot lately that cyber is now the highest legal risk for an organization. How is that possible?

Amy S. Mushahwar: We used to just have a very predictable cycle of notifying individuals, providing credit, monitoring insurance, and then bracing for maybe there was a little litigation, maybe there wasn't. In today's modern attacks, you have several cycles of attack. You might have an entire system lockup that makes it so you can't undertake business. A cybersecurity event is essentially, if you can't undertake business, a cash flow event. Those cyber events are your largest risk because in addition to losing consumer trust, which that's been for the entire cycle of data breaches, regardless as to whether or not it's a newer ransomware or data ransom, now you have the extra added specialness of perhaps not being able to intake cash, not being able to service customers, and losing more trust as an organization.

Ken Fishkin: If there were a few things that you could tell somebody on how to mitigate some of this risk without bringing all the lawyers in yet, what would those things be?

Amy S. Mushahwar: So, I'm going to say multi-factor authentication, multi-factor authentication, multi-factor authentication. Did I say that loudly or enough? It's important. It's important that you have it. It's important that all your vendors have multi-factor authentication.

Now, that said, MFA alone doesn't indeed fully secure an enterprise. We do want to make sure that you're patching—that is both software patching and hardening configuration management. We want to make sure that you are attending to your security dashboarding. We want to make sure that you have EDR, or endpoint detection response, software installed as an organization so, if you have perhaps a ransomware malware, it doesn't creep and crawl across your network—it can stop at 1 or 2 machines.

And we do want to make sure that as an organization, you are requesting and reviewing artifacts of security compliance, so you know the status of your security program, and you have ready artifacts of compliance that you're reviewing, that you're sharing with your general counsel to make sure that everybody's aware of where you stand as an organization.

Ken Fishkin: From a cyber legal perspective, what are some of the lawyers' roles and responsibilities?

Amy S. Mushahwar: Let's start pre-incident, because that's where we hope where we are. Before an incident, a lawyer is key in ensuring you have an appropriate and proper program. But it doesn't just mean the lawyers drafting the policies or getting a firm to drop the policies, but you're ensuring you have policies, ensuring you're generating appropriate artifacts of compliance to show implementation of those policies.

You have workflow and you have budget and governance. So, on the lawyers' role, you know, we really are the bastions of making sure that you can show appropriate and proper implementation and that policies don't just sit should sit on a shelf collecting dust on incident response side. The lawyer really ends up being the quarterback of the incident response team, working with the Chief Information Security Officer. We make sure that, both in-house and external counsel, we work to hire third-party experts so they're under privilege. We are second check on the forensics process, especially as outside counsel. And we're monitoring for legal risk, maintaining timelines so we can show defense ability of our actions, when now, especially if you have PII, you're going to have ensuing lawsuits.

Ken Fishkin: Ransomware has evolved over the past year or so, where they're not really encrypting data anymore as much. They're taking the data and they're not disrupting business as much, so there's less incentive to report breaches because of that. They're stealing the information, but they're not bringing down the whole business. So as a result, internal lawyers might put a lot of pressure on the CISO to report that incident. What are your feelings about that?

Amy S. Mushahwar: Well, first of all, if data was taken and it's a simple data ransom, you have to report in accordance with law. So in the event that PII leaves the building, paying the ransom doesn't negate the legal analysis, and the fact that access and or acquisition occurred. So that's what I want to say is just a square one.

I hear you that CISOs are under increasing pressure, that if there is an argument that data access or acquisition did not occur, we want to lean in on the argument that, you know, avoids reporting if it is defensible. For me, the key is if it is defensible, you know, there are lines that we can't cross and that CISOs don't want to cross, because if an acquisition or access to data, depending on the legal regime in which you're in occurs and we don't report it, and that issue compels, you know, we could we could have another issue and you just don't want to be there.

We don't want to be there in terms of personal liability for CISOs knowing many who are getting their own liability insurance policies. You don't want to be there as the General Counsel that helped make the CISO call, but we want to fall on the right side of the law. If the right side and the right legal analysis creates a defensible position where data was not accessed or acquired, then it's not a breach. It's a mess. And it would support not reporting something that didn't end up having an access or acquisition of data.

Ken Fishkin: Let's say you're a General Counsel and you want to get a better handle to make sure of the company's cybersecurity posture. What are some of the things that they could do to make sure that they have a little more comfort?

Amy S. Mushahwar: I know that we've talked about artifacts of compliance, the first being just don't assume that a CISO has, or a Chief of Security has, everything handled because they are under time constraints, budgets, staffing constraints. So GCs, first have that good relationship and conversation with your CISO to make sure that you know his or her pain points, and you can help them get effective resources if they need an advocate.

The second being, you know, the CISOs are our excellent experts, but sometimes just having the view of a CISO presenting artifacts of compliance and reviewing their security program just gives another second opinion. And General Counsel, their function is to make sure that you’re staffing effective legal management of operational functions and security.

We want to make sure that as lawyers, if you're not collecting artifacts of compliance and have a compliance folder in addition to an audit folder for your cybersecurity environment and privacy environment, you need to start to. And if you don't know where to start, that effective outside counsel that can help you create your evidentiary folder, so you know where you stand in terms of cybersecurity. And if a regulator were to ask for objective artifacts of compliance, you know what would be looked at.

Ken Fishkin: Going from small organizations to much larger ones like SAS providers, what are some of the challenges that they face dealing with business-to-business vendors?

Amy S. Mushahwar: Downstream vendor management is a problem for all large SaaS companies, and particularly a problem if any of your vendors have access to your data plane, that is your customer data plane. SaaS providers and big vendors, they have customers who are often large fortune 500 companies that are just as powerful as they are, who could sue them. And you know, when you look at vendor management and those who have access to the data plane, oftentimes those vendors are smaller, add-on vendors and may not be able to take the size of hit that a large SaaS company has to take from its big premiere vendors. So, you know, that downstream vendor problem is just amplified versus providers with thousands of clients.

Now, that said, at base, a SaaS provider's biggest problem when you have been compromised is that you have thousands of clients that can sue you. So just scaling incident response management and making that a mass communication event, effectively managing it to scale with the business teams and corporate communications and making sure, especially for public companies, that your public messaging, your customer messaging, your investor messaging and your downstream consumer messaging are all together. Because oftentimes SaaS providers have business-to-business lines and consumer lines, so there's often multiple different messages and messaging that needs to occur at the same time, but also prioritizing those big business-to-business clients where you want to make sure that you are taking care of those relationships, even in a breach.

I always call it a “breach as a service.” It's breach of customer service, and it's a customer win-back event if it's handled well. Because an incident in and of itself is a moment for pause for all of your clients: “Do I still want to continue to do business with this company?” And you want to go through a breach as a SaaS provider with all your customers emphatically saying, you know, he didn't like the fact that this breach occurred, but they handled it really well, and that's a customer win back event.

Ken Fishkin: What do you recommend with what just happened with this event that we're talking about that regular customers can do to protect themselves, if anything?

Amy S. Mushahwar: Salesloft and the Drift event—even though it was AI and an AI-based CRM customer service integration, it's all of the integration and cobblestoned integrations that we face as companies. You know, you've got a Salesforce instance with multiple integration partners. You have a Google instance with multiple integration partners.

First of all, know thine integrations, and, you know, where you have those secure connections so, you know, you're not fumbling for a few days going, "Okay, do I really use this product? Who do I check just to know who I use this product?" So have your vendors map so someone can either swiftly go into IT, swiftly go into Procurement, double-check that someone's a vendor and know whether or not you're impacted.

Also, a corollary to that is beware of shadow IT and make sure that you, you know, in the event that you find shadow IT and shadow integrations, that those get documented, so you can respond quickly and be able to communicate quickly and know whether or not you're impacted, and you don't waste days fumbling and trying to determine you're not impacted, and then ultimately discover events.

So, because many of our breach issues may not necessarily be your infrastructure issue with the infrastructure of your vendor, making sure those catalogs are just extremely important and something that always falls by the wayside when folks have thousands of vendors. So, it is a never-ending battle but it is a battle that you must resource, because then you can respond effectively to a Salesloft or to a SolarWinds. Because if you don't have those vendors categorized, you spend needless days, needless hours trying to figure out what you have and where it is impactful instead of having it cataloged.

Ken Fishkin: Well, Amy, it was an absolute pleasure having you.

Amy S. Mushahwar: Thank you, and happy Cybersecurity Awareness Month everybody!