Lowenstein Sandler's Cybersecurity Awareness Series

Session 5 -
How Patching log4J Can Mitigate Regulatory and Insurance Issues

By Mary Hildebrand and Ken Fishkin
JANUARY 2022

Ken Fishkin: Hi, I'm Ken Fishkin. And today I'm with Mary Hildebrand Partner and Chair of Privacy and Cybersecurity. And this is another segment of our or security series. And the first question I'd like to ask you, Mary, is what should companies expect if they don't adhere to trying to deal with this log4J problem?

Mary Hildebrand: Well, first of all, thank you for having me. It's a pleasure to be here. I think that a company ignoring the existence of this issue would be very ill advised. Some of the consequences could be, of course the first one you might think of as a data breach which could expose the personal information of customers, employees, and third parties, with whom the company has a contractual commitment to maintain data in privacy, in confidence. We could also have issues associated with obtaining or executing on a cyber insurance policy. If there's a data breach one of the underpinnings of any insurance policy is that the insured comply with applicable law. Data protection laws in the United States and around the world to have two sides, it's like two sides of the same coin.

One side is privacy protections, and the other is cybersecurity. Many of those laws require that companies execute reasonable care in selecting the security measures they employ. And for example you know, installing patches on a regular and methodical basis. But what is reasonable is usually not specifically defined because the technology changes so quickly and there are other factors impact what it reasonable; the nature of the data, where it's stored, how much access to the data is required, what the purpose of acquisition was. And also factors in, you know, what measures are reasonably available to a company to protect the data. So there's a lot going on in making those decisions of what is reasonable and how to comply with the applicable data protection laws and a company and their insurance provider may not see eye to eye on exactly what that is.

Ken Fishkin: Thank you, Mary. You know, as this evolves the regulators are getting involved and the FTC in fact, put out an advisory on January 4 saying that if you don't take reasonable care, then uh, there will be penalties potentially. And what are your thoughts, what are some other regulations that our clients should be aware of?

Mary Hildebrand: Ken? I wouldn't call it a memo. I would sort of call it a shot across the bow. The FTC was really advising the world that they intended to exercise all of

their authority under regulation 5 to protect consumers from unfair and deceptive trade practices. And that would include, of course, ensuring that companies use reasonable steps to mitigate known vulnerabilities. I don't think it's an issue that this is a known vulnerability and that it would be, I don't want to say negligent, but it would be surprising if a company didn't take steps to mitigate. Other laws that could be relevant are the Gramm-Leach-Bliley Act for non-public personal information held by financial institutions, Healthcare data in entities and organizations governed by HIPAA. We also in the United States now have a number of data protection laws at the state level, including of course, most notably California. Soon to be followed in 2023, by Colorado, Virginia, and of course we've still had Nevada for several years as well and others are pending.

I might add that the regulators here, the FTC, and others have to take the lead because the United States is one of the few major powers without a comprehensive national data protection law. There also have been some other repercussions that I probably should mention here, which is that this particular vulnerability is open source and commentators, including the FTC, have pointed out that open source is maintained and supported typically by volunteers. So it is a particularly unregulated area. However it is critical to the operation of, I would venture to say, millions of different companies. There's a long trail here. Everyone seems to agree that it's going to take a while for the repercussions of this vulnerability to die away. And I should also note that nation state actors have been very involved. Although from what I understand, Ken, it doesn't take a tremendous amount of skill to exploit this vulnerability. So there's lots to be careful of and very good reasons to take steps to mitigate.

Ken Fishkin: Yeah, we can definitely see, uh, this vulnerability not being resolved within this year. It's gonna be… <laugh>

Mary Hildebrand: No, no, not a chance in the world.

Ken Fishkin: a few years. I know everybody's working, feverously hard to patch and then patch again and then patch again. And we were talking last time about having to deal with asset management to help you take care of you know, understanding where your assets are, and also performing tabletop exercises in the event that you are breached, but what are some other legal actions that companies should take? If they want to be proactive?

Mary Hildebrand: There are lots of them. And to rattle off a list might not be productive. Why don't we start with what should come first? The key phrase you used, I think, Ken, was asset management. And one way to look at this is to view the data itself as an asset of the business. The first step should be to do an inventory of the data and the personal information that your company collects and processes because it is, seems obvious to say it, but you can't manage and ensure that anything is properly regulated unless you know what you have, what you have it for, where it's located. And what some of the business procedures are that surround that asset in this case, a data asset. From there one would to determine what data protection laws impact that data and

impact your business. And then you begin the complicated process of integrating those data protection laws into day-to-day operations.

Ken Fishkin: Well, thank you, Mary. And this concludes another episode of our Cybersecurity series. Thank you.