Barclay Damon Live Presents: The Cyber Sip Podcast

Episode 7: "All of Those Media Stories About Cybersecurity–What Do They Mean?"

Speakers: Kevin Szczepanski, Barclay Damon

[Kevin Szczepanski]: Hey, everyone, this is a Barclay Damon Live broadcast of Cyber Sip, practical talk about cybersecurity. I'm your host, Kevin Szczepanski.

Let's talk. Welcome everyone back for another episode of Cyber Sip. Today, we're going to talk about media stories about cybersecurity. What do they mean? But before we get started, I just want to take note of the obvious--we are in blazing sunshine here in our beautiful downtown Buffalo Barclay Damon Live Studios. We are here, as I said, to talk about media stories about cybersecurity. What do they mean? The reason I wanted to talk about this today is because, if you're like me, you are inundated with the latest stories about cybersecurity.

They come across your screen by the dozens every week, sometimes every day, and it's sometimes difficult to make sense of them all. And so I thought about doing an episode that would take a couple of these stories and use them as examples of how we can take away information, practical tips from many of these cyber stories that we see along the way. So we're going to talk first about Log4j, and we're going to talk second about FTC's recent amendments of the Gramm-Leach-Bliley Act safeguards rule. So let's take each of them in turn, and I want to talk first about the story and then about the practical takeaway.

So what's Log4j? All you need to know about Log4j is that it is in the words of FTC, a ubiquitous software. It is used in numerous consumer facing software programs. Amazon uses it, Apple uses it, Twitter uses it.Chances are if you've been online, you have encountered, whether you know it or not, Log4j software. Recently, and just fittingly, for the Christmas season, a vulnerability was discovered in Log4j; it's a big problem because of how prevalent that software is and so many applications.

And essentially, the vulnerability enables threat actors to take control of a computer or computer system, access data and potentially even deploy ransomware. So it was a big problem, and understandably, there was a lot of media reporting about it. And helpfully, FTC came out with some high points, bullet points of how to respond to the Log4j vulnerability. I just want to read to you the three key bullet points FTC published around the holidays, and then I want to talk to you about it.

So here they were. Here's what FTC told consumers and businesses across the country. First, update your Log4j software package to the most current version found here, and then there's a link to that updated version. Second, consult CISA, or Cybersecurity and Infrastructure Security Agency guidance to mitigate this vulnerability.

Third, ensure remedial steps are taken to ensure that your company's practices do not violate the law. Failure to identify and patch instances of this software may violate the FTC Act, so that comes from the FTC. Again, very helpful information, but the question--if you're like me becomes "What does all of this mean?" What FTC

is essentially saying: is deploy the patch and conduct a security review. What does that mean? To talk a little bit more about what it means, I'd like to use one of my favorite metaphors, and that is the metaphor of the unlocked house.

So let's say I'm out and about on a weekend day running errands, and I come back after several hours to find that I have left my front door unlocked and open. What's the first thing I'm going to do? I'm going to walk in the door, close it behind me, and lock it. That's the patch. You're going to deploy the patch to fix the glitch. Close the gap, if you will, to make sure that that vulnerability no longer exists. And that's what I've done when I've walked in close the door and locked it behind me. I have eliminated the vulnerability. No one can come in from that point forward. But. I'm not in the house for very long before I start thinking to myself what happened while I was away? Did someone come in? Where did they go? What did they look at? What did they take with them before they left? And that is the analogy to the security review. So just like I'm going to walk around my home upstairs, downstairs in every room to make sure everything looks to be in its place, nothing's been taken or disturbed. You're going to want to conduct a full-on security review of your physical electronic safeguards to make sure that whoever got into your system did not deploy any malware, ransomware... did not deploy any devices that could be used later to access or exfiltrate data.

So you read the FTC guidance, you hear stories about Log4j. There are a lot of them; they can be confusing. The guidance itself is almost ominous, reminding us that we need to make sure that we comply with the law and that failure to do so can subject us to penalties for violating FTC.

So what's the key takeaway from all of the stories that we're hearing and reading about Log4j? First and foremost, patch the vulnerability. And second, make sure you conduct a security review to make sure that nothing bad happened in your system before the day you patched it. Now, the second story I want to talk about is one that has just come out, and I want to give kudos to Shardul Desai. And Mr. Dhesi, I hope I'm pronouncing your name correctly. But Shardul Desai, just did a great piece in Law360 about the FTC's recent amendments of the Gramm-Leach-Bliley Act safeguard rule. And that is the rule now requires FTC-regulated entities to implement particular cyber safeguards. Now, if you're like me, you see a fair amount of these pieces and there is the alphabet soup of regulatory agencies, whether it's FTC or SEC on the federal side or DFS, the Department of Financial Services on the New York state side.

All right. So we see this story about FTC amending the Gramm-Leach-Bliley Safeguards rule, and we think to ourselves, "I'm not regulated by FTC. This isn't something I have to pay attention to." Or is it? Well, there are a few reasons why I think you do.

First, and it goes without saying, if you are regulated by FTC, you do have to comply. Second, even if you're not directly regulated, if you're doing business with an entity that is FTC-regulated, you may have to comply either by law or by whatever vendor contract you have in place with that regulated entity.

But there's a third reason why we should pay attention to federal and state regulators implementing cybersecurity safeguards. And that is, regulators are not devising standards on their own. They're not really creating anything new. These federal and state regulatory standards very often reflect existing industry standards and best practices. So it's a really good idea to look at what federal and state regulators are doing, because very often they reflect the emerging trends for cybersecurity across the country and across many, if not most, industries. So what's the takeaway here? If we were to shine the light of blazing sunshine on all of these media reports, what do we conclude? Well, I think there are three key points that we can all keep in mind. First, conduct a cybersecurity review. Knowing what your organization's physical and electronic vulnerabilities are up front puts you in the best position to prevent and to reduce the threat of a cyber attack.

Second, implement and be sure to update your organization's cybersecurity policy; That combination of physical, electronic and even legal safeguards that you have in place to protect your organization, your employees, your data, and your consumers. Third, put in place an incident response plan. We talked about

IRPs in one of our recent episodes with Mike McCartney of Avalon Cyber. And if you'd like to learn more about that, you can check out that episode on barclaydamon.com. So what do these media stories about cybersecurity really mean and how can they help us?

Well, I think each of them is important in its own right. But the big picture is they remind us to be vigilant in our physical, electronic and legal safeguards. And if we all do that, they'll upgrade our cyber hygiene and do the best we can to prevent the next cyber attack.

I hope you found this episode helpful. I look forward to seeing you on the next one.

The Cyber Sip podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.