Linn-Freedman – EMCS Podcast Series – Rise of the Third Party Vendor Threat

JO LEE: Welcome to Brown University's Cybersecurity News podcast. I'm Jo Lee, Program Content Marketing Director. I'm proud to welcome Linn Freedman, a partner at the law firm Robinson+Cole. Linn chairs the firm's data privacy and security team and is a faculty member in the Executive Master in Cybersecurity program.

Linn, the Ponemon Institute recently released the findings of its survey, Data Risk in the Third Party Ecosystem. What findings from this report were you most concerned by?

LINN FREEDMAN: So first of all, the Ponemon Institute comes out with reports periodically. And they're very, very good. I would highly recommend that you follow them.

But in particular, in the industry right now, we're seeing that third party vendors are a high risk area for companies. And this report confirms that fact.

And the interesting thing that we're seeing in the industry is not only is this a high risk area, and we're seeing more and more data loss from third party vendors as opposed to companies, we're also seeing a break in the communication between the company and their third party vendors.

In other words, the Ponemon Institute's most recent report indicates that companies don't believe that their downstream vendors will even tell them when they have a data loss, which is surprising and concerning. And also they don't believe that they know all of the companies downstream from their first party vendor who has access to their data.

And we're seeing that in the industry. And that's why vendor management is such a very important part of the risk management that you do when you're looking at your data privacy and security program. You have to know where your data is. You have to know what vendors have access to it. And you have to make sure that they have appropriate privacy and security measures in place for your data.

JO LEE: Can you tell us about some third party vendor crises that have occurred?

LINN FREEDMAN: Really the one that everybody knows about but a lot of people don't even know the details of was the Target breach. Which which was the first data loss and data breach that really rocked the world when it came to third party vendors having access to data.

In that particular case, in case you don't know, the third party vendor was the HVAC vendor that was in charge of the environmental controls of all of Target's retail stores. And what happened was that a hacker got into the third party HVAC vendor's system, was able to get the credentials to get into Target's IT system-- just to put this very simply-- and Target did not segregate their environmental data from their customer data. And so the hackers were able to get into the customer data.
That was the first one that companies found out about. And obviously as soon as people found out about that, then everybody rushed around to find out what credentials their third party vendors had. But we're seeing data loss more and more with third party vendors through websites, through access to data, through credentials.

Your weak link is really your third party vendor. And the weaker link is all the vendors that that vendor has, that is either disclosing your data to or giving access to your data. So third party vendor management right now is something that we're concentrating on really hard with our clients.

Because again, if you don't know where your data is, and you don't know what your vendors are doing with it or the security measures that they have in place, it's a weak link in your risk management program. So find out where your data is going, keep track of your vendors. That's called a vendor management program. A lot of times that's something that you can do through--you must really do through contractual provisions. And make sure you have a contract in place. And make sure you know where your data is going.

JO LEE: The survey talked about the need to have responsibility for third party management. It's often very distributed throughout the organization. Can you talk a little bit about trends towards consolidating that or dealing with this issue?

LINN FREEDMAN: So really, best practice around vendor management is to have one person own that program. And it doesn't really matter, and it differs from company to company. So it could be in legal, it could be in finance, it could be in compliance.

What I will tell you is I don't recommend that it sits in IT. It should sit in the compliance or the legal department. Because one of the things you have to do is follow your data. IT can help with that. Finance can help with that. But you want to make sure you have contracts in place. So in the event of a data loss, you have contractual provisions and indemnification in place. So whether it sits in legal or compliance doesn't really matter to me.

But there should-- finance and IT should all be part of the vendor management program. Because IT, a lot of times, is the one who's sending the data. You want to make sure legal and compliance know when data is leaving the organization.

And then the way to kind of wrap it all up is through finance. Because I recommend that if that vendor doesn't have appropriate measures in place, and you do your security risk assessment, and they don't sign the agreement with you that says that they have appropriate measures in place and they're going to indemnify you, then they don't get pay or they don't get your data. It's a really good way to get companies to pay attention to your contracts and to the obligations that they have to keep your data private and secure.

So it should be-- the different departments that should be included are legal, compliance, IT and finance at the minimum. But it should be owned by one of them.
JO LEE: You just provided a great summary of best practices. But before we end, any other best practices that you want to mention?

LINN FREEDMAN: Really, the first part of vendor management is mapping your vendors. Just like organizations do data mapping to find out where their data is in their organizations so they can implement their privacy and security plan, we strongly recommend that you map your vendors. And in large organizations, that's hard to do.

But you need to be able to figure out who your vendors are who are getting your highest risk data. So that you can make sure that you can audit them for their security protocols. And that you have contractual provisions in place.

So data mapping and vendor mapping are two very important tools in this process.

JO LEE: Thank you Linn for sharing your thoughts on this subject. For information on future podcasts, program news, and upcoming events, visit brown.edu/cybersecurity.