Podcast Transcript

2024 DSIR Deeper Dive: Deeper Dive into the Data

Date: July 23, 2024

Guest: Elise Elam and Courtney Litchfield, **Host:** Amy Kattman

Run Time: 15:45

For questions and comments contact:

Elise Elam

Associate
Cincinnati
T: +1.513.929.3490 | eelam@bakerlaw.com

Courtney Litchfield

Associate
Chicago
T: +1.312.416.6236 | clitchfield@bakerlaw.com

Kattman: On April 23rd, BakerHostetler's Digital Assets and Data Management Practice Group released its annual Data Security and Incident Response, the DSIR, report. This year marks the 10th anniversary of the report, which is now widely used by businesses all over the world to help develop their cybersecurity measures, incident response plans, and information governance practices. I'm Amy Kattman, and you're listening to BakerHosts.

We're back with a Deeper Dive series covering key topics in this year's DSIR. On today's episode, we will take a deeper dive into the data and trends of our 2024 report. Our guests today are Elise Elam and Courtney Litchfield. Elise is an associate on our Digital Risk Advisory and Cybersecurity team, and Courtney is an associate on our Healthcare Privacy and Compliance team. Both are co-editors of the DSIR report. Welcome to the show, Elise and Courtney.

Litchfield: Hi, Amy. Thank you for having us.

Elam: Thanks, Amy. Happy to be here.

Kattman: Elise, let's begin with network intrusions. What did our incident response team see with this type of incident last year?

Elam: Network intrusions were the number one type of incident that we handled last year, and the prevalence was driven in part by an increase in ransomware activity as well as some pretty notable attacks on file transfer platforms that impacted a large number of organizations. And what we're seeing is that threat actors are using multiple different tactics to get into victims' networks, but they're still using the same tactics they've always been using all along. Phishing, social engineering, open RDP, and other vulnerabilities in, for example, remote access tools and like I mentioned, SFTP systems.

And in fact, about a quarter of the network intrusion matters we handled last year were caused by an unpatched vulnerability. And some of these were a zero-day vulnerability that the threat actor was able to exploit before a patch was made available. So, something that hadn't been known to the company prior to the threat actor using it to gain access to their system, but most of the time they were caused by a vulnerability for which a patch had already been available for some time. And so really, there is no silver bullet for preventing network intrusions, but it is critical that, among other things that we'll talk about later, companies have robust patch management programs and policies in place to help prevent these types of incidents.

Kattman: Thanks, Elise. Courtney, what happens after a network intrusion takes place?

Litchfield: So, ransomware is deployed in nearly three quarters of the network intrusion incidents we handled last year. In over half of those matters, the threat actor stole data from victims or our clients' networks. The good news is that companies, they've become much more resilient. So, they're detecting and recovering from incidents more quickly than before, and even though the average ransom amount paid has been increasing, overall, companies are still paying that ransom less frequently. So, in 2022, about 40 percent of our clients paid a ransom, while in 2023, only 27 percent paid. This is in part due to higher demands but also because of our clients having viable backups and also access to those backups.

That said, containment is taking longer. So, on average it took our clients about five days to contain an incident from when they first detected it. The threat actor group called Scattered Spider is partially to blame for this increase. Scattered Spider, they are known to try to get back into a network after being kicked out, which of course makes containment more difficult and more time consuming.

Finally, several weeks after network intrusion matters, we often see notification individuals, so whether that is going to be employees, customers, patients or others. Overall, the number of matters that result in notice has remained pretty

consistent with notice occurring in about 40 to 45 percent of matters. However, the size of the notice population has nearly doubled. So, in 2022, the average number of people notified in a matter was just under 50,000, while in 2023, this number was just under 100,000. We've said this in the past several DSIR reports, but removing old data is extremely necessary. Additionally, organizations need to ensure that their workforce are not creating documents containing an unnecessary amount of personal information. For example, if you're extracting a report that has names and dates of birth and Social Security numbers, maybe replace those names with a unique identifier or only do the last four of the SSN, something like that to help limit the overall amount of data that is in a document.

Kattman: Courtney, would you talk about how threat actors are adapting to companies increasing their safeguards?

Litchfield: So, as organizations adapt, unfortunately the threat actors are too. It is like a game of Whac-A-Mole. Once you cover one gap, another one just pops up. For example, threat actors are sending phishing emails as dot RPMSG or encrypted emails, which gets through even the most conservative spam filters.

They are also doing what we call living off the land, which means they're using a company's existing and approved tools to facilitate their attacks. This makes it much harder to detect the unauthorized activity. Threat actors are also using social engineering to call a help desk to reset a user's password. So, just over the past few months I've had a number of matters where a threat actor was able to bypass the help desk verification process, which often involves asking for the person's name. It might involve asking for their user ID but then also their date of birth or the last four of the SSN, and because that information is largely publicly available, threat actors are able to use that and get past that verification process in order to reset the password.

We also are continuing to see MFA bombing. This happens when a threat actor attempts to log in so many times in quick succession that the user is just getting hit with MFA prompts over and over and over again, and they either inadvertently approve the request or just to get it to stop, they'll do it.

Elam: Yeah. And I'll also add to that that if a vendor of yours has an incident, following up with them post incident to learn more about the attack and what the company has done following the incident to improve their security is really important as well.

Kattman: So, Elise, what steps do you recommend companies take to combat these threatening tactics?

Elam: Well, as always, having an EDR tool globally deployed and properly configured is critical. This has made a huge difference in our clients' ability to respond to an incident quickly. And one thing that gives a benefit there is that it helps with containment as well as speeding up the forensic investigation. So, the timeline that Courtney talked about actually can be condensed if the EDR tool is in place, but that also helps prevent the incident in the first place as well.

It is also super important to have MFA and to have that configured correctly and to have a patch management program as discussed before. And then for email access, companies should do four main things: using conditional access policies, shortening sign-in frequency, restricting ability for users to add approved MFA devices, and then of course regular training. And I'm going to discuss each of those in more detail.

Using conditional access policies to only allow specific devices to connect to the email tenant is really important, but those conditional access policies can also be used to enforce other controls, for example, geo-blocking. So, you can limit the IP address location that is signing into a certain account. So, if all of your employees are based in the U.S., for example, and they don't travel frequently, you could consider limiting the geolocation to only U.S.-based IP addresses. You can also use those to block legacy authentication protocols, which is really important, and then you can also use conditional access policies to limit sign-in frequency. And what that means is essentially you require users to reauthenticate more frequently. So, it could be once a day, once every four hours, or even every time the user attempts to access a certain resource, including email account. Also, companies should restrict the ability for users to add approved MFA devices.

One thing we're seeing happening is that threat actors, once they gain initial access into an email account, they maintain their persistence by adding their own device to the approved devices able to receive MFA prompts. So, then when the threat actor goes to log into the email account again, the threat actor themselves are getting the MFA prompt. And then they can approve it, and that allows them to stay in the account undetected because the actual user won't be getting those prompts.

And then, of course, training, as always, is very important. Regular training on how to identify phishing emails and what to do when one is received as well as training on appropriate MFA practices. So, for example, what to do or not to do when receiving unexpected or a large number of MFA authentication requests. And Courtney talked about MFA bombing. This is one thing that we're seeing more frequently, where if the threat actor is just initiating the MFA prompt over and over and over again, what you should train your employees to watch out for that and to know that they should not approve those MFA prompts if they don't believe they're the ones initiating it.

And then just generally speaking, especially for network intrusions, organizations need to have and regularly test their backup solutions, and those backup solutions should be air gapped and immutable. What that means is that if a threat actor gets in and encrypts your network, then the data on those backups, because they're separated from your network, won't also become encrypted. And they're immutable, which means they can't be changed, so they can't be deleted by the threat actors if they somehow get access to those backups. Threat actors know the common providers for backup solutions and search in a keyword search for those companies and can very quickly locate backup repositories. And one thing that those threat actors do to place additional pressure on companies

to pay is that they delete those backups. So, if they're immutable, they can't be deleted. And while having a good and well-tested backup solution won't actually stop an incident from occurring, it can greatly reduce the impact of one and can increase the speed with which a company can get back up and running after an incident occurs.

Kattman: Well, as I hear from both of you, these intrusions are constantly evolving. I'd like to ask one last question of both of you. What do you think the data will look like next year? Courtney, let's start with you.

Litchfield: It is a good question, especially what you just said, these network intrusion matters are evolving, and really just the whole scope of cyber-attacks in our practice really evolves all the time. So, it is a tough question to answer. But if you look at just our most recent DSIR report with respect to incidents that occurred at a third-party vendor, the number of matters we've had that involved a vendor represented a fourth of those that we handled in in 2023, which that is a huge increase. When you compare from 2022 to 2023, it went from 16 percent to 25 percent. This was in large part due to the May 2023 incident at SFTP provider MOVEit that Elise mentioned earlier. But if you look at the high-profile incidents that have already occurred this year between Change Healthcare and many others, we expect the percentage of incidents that will occur at a third-party vendor, it will continue to be elevated if not even higher than that 25 percent marker.

And just to add to that list that Elise gave you on steps that organizations can take, also important is to vet third-party vendors. It is really critical to do that both at the outset but then also as you continue your relationship with these vendors. This is often overlooked, but it is equally important. You need to initially vet and then also re-vet. So, by exercising ongoing diligence you can request updated security assessments, review contracts for any updates that need to be made, and then also continue to confirm that the data, if any, is being held by the vendor, that data is being offboarded or deleted if it is no longer necessary.

Elam: And also, with respect to the types of incidents, I think we expect the hierarchy of those incidents of frequency of the different types of incidents to be very similar to this past year's report. I think network intrusions are going to continue to be the number one type of incident that we see followed by business email compromises probably coming in as a close second.

For network intrusions that involve ransomware, I think it is pretty likely the total number of matters that result in payment of a ransom will be lower this year than they were last year. And that is the trend that we've been seeing is that the frequency of payment has been decreasing, and that is due in large part to our clients maturing in their cybersecurity posture, having better backups and therefore not needing to pay as frequently to get back up and running following a ransomware incident.

Additionally, the healthcare industry will continue to be the most impacted industry overall, especially thanks to the Change Healthcare incident that we mentioned before that has impacted a lot of our healthcare clients already.

Kattman: Thank you so much, Elise and Courtney, for joining us today.

Elam: Thank you, Amy.

Litchfield: Yeah. Thank you so much for having us. We're happy to be here again.

Kattman: If you have any questions for Elise or Courtney, their contact information is in the show notes. As always, thanks for listening to BakerHosts.