Podcast Transcript

2303 DSIR Deeper Dive: Deeper Dive into the Data

Date: August 9, 2023

Guest: Elise R. Elam **Host:** Amy Kattman

Run Time: 11:02

For questions and comments contact:

Elise R. Elam

Associate
Cincinnati
T: 1.513.929.3490 | eelam@bakerlaw.com

Kattman: Managing digital assets requires the efforts of the whole enterprise. The 2023 issue of the Data Security Incident Response Report, or the DSIR, includes more content than ever regarding the data ecosystem and how companies can best manage their digital assets as they move through the life cycle of data. The DSIR, of course, dives deep into the annual incident response trends and analytics our clients and friends depend on. It also covers topics such as global privacy, ad tech, the increase in litigation, healthcare privacy and compliance, and the latest in emerging technology.

I'm Amy Kattman, and you're listening to BakerHosts.

We are back with the Deeper Dive series covering key topics in this year's DSIR. On today's episode, we take a deeper dive into the data and trends of our 2023 report. Our guest today is Elise Elam, an Associate on our Digital Risk Advisory and Cyber Security team.

Welcome to the show, Elise.

Elam: Thanks, Amy. Happy to be here today.

Kattman: So, I'd like to begin with ransomware. Elise, what notable trends have you been seeing over the last few years?

Elam: That is a great question, Amy. So back in 2018, we started seeing a really large increase in the average ransom that organizations were paying. And in 2021, this number actually decreased for the first time in the history of our report. But then

last year we saw this number go up again. The largest ransom demand received across all of our matters that we handled in 2022 was over $90 million, and the largest amount paid was over $8 million. The average amount paid was just over $600,000.

Another trend, unfortunately, that we saw, was that recovery times were increasing, meaning it took longer for our clients to recover after facing a network intrusion or ransomware incident, and that trend actually nearly doubled for some industries compared to 2021, and some industries even faced an average of about two and a half weeks to reach a level of acceptable recovery after the encryption event occurred.

Kattman: Elise, what industries are most affected?

Elam: Honestly, all of them, although our data shows that regulated industries such as healthcare and finance did face shorter recovery times. These industries have had to follow cybersecurity laws and regulations at both the federal and state levels for quite some time now. Other industries are catching up, but there is still a lot of work for them to do.

Kattman: So how can companies take action and be more resilient against network intrusions?

Elam: Well, there are lots of things that organizations can do to be more resilient, and I tend to think of them in three sort of broader categories that companies should focus on: prevention, preparation, and mitigation. And some things can sort of go across all three, but it is important to take measures not only to prevent a cyber security incident from occurring in the first place, but also to plan for and practice what to do in the event one does actually occur. And it is also really important to take measures that will minimize any impact the incident may have on a company's systems or to its data. So, in other words, if an incident does happen, making sure it is not a catastrophic incident, shutting down the entire company, or losing lots and lots of data. There are measures that companies can take to sort of minimize that harm even when something happens.

A key differentiator we see in companies that experience network intrusion events and those that don't, or those that experience more significant intrusion events and those that experience more minimal events, is the wide deployment of a correctly configured endpoint detection and response tool, or an EDR tool, with around-the-clock internal or external monitoring. And another key thing with EDR tools is to make sure that the anti-uninstall feature is enabled. We've seen threat actors find ways to uninstall the EDR tool from certain devices, allowing them to essentially bypass the security measures that a company has put in place.

Also, especially for critical systems and data, companies need to make sure they have immutable backups. We've seen threat actors delete non-immutable backups, which can force companies into a position where, even though they had

backups prior to an incident, they may have to consider paying a ransom to recover key systems and data in order to get back up and running.

Also, really important is to practice recovering from backups. It always takes longer than expected, and technical issues can unexpectedly arise. So, it is better to go through the process prior to an incident, when you're not responding in real time to the incident, so you can take the time to understand the work involved in actually restoring from backups.

Finally, it is really important to prepare and train. In other words, conduct tabletop exercises that involve all the teams that are included in the company's business continuity and disaster recovery plans so that all of these different teams can get a sense of what it is like to need to work together on making plans for recovery and other critical items that occur during an incident response.

Kattman: So last year, fraudulent fund transfers were a really hot topic. What can you tell us about these trends in 2022?

Elam: Well, Amy, actually last year we saw an overall positive trend related to fraudulent fund transfers, although we did handle a lot of matters related to fraudulent fund transfers, the total amount of funds transferred in 2022 was almost half what it was the prior year, and the average transfer amount was almost $450,000 less than it was in 2021.Unfortunately, though, only 24% of matters resulted in recovered funds. So, what that means is that less money is being stolen, but that money is recovered less frequently. And a key differentiator here in whether or not funds are recovered, or how much of those funds are recovered is just timing. The faster you identify this issue, the more likely it is that a company is going to get at least partial funds recovered.

Kattman: So even though it is happening less frequently, could you still provide us with some tips for preventing fraudulent fund transfers?

Elam: Definitely. There is always things that can be done to decrease the likelihood of fraudulent fund transfers from happening. These mostly occur through what we call business e-mail compromises, so it is important to implement and enforce multi-factor authentication or MFA for remote access to e-mail. And code-based MFA where you have to enter a number or text-based code that is texted to your phone, something like that, is better than a push MFA notification where you get a pop up on your phone and you press the button to accept it. So, the code-based MFA is better because it requires an extra step to enter the code into the authentication screen. And this is important because more and more frequently, we are seeing threat actors use a tactic called MFA bombing, where the threat actor just keeps sending authentication requests over and over and over and over again, which causes the person receiving those authentication requests to become overwhelmed or fatigued or frustrated, and they just allow, hit the authentication, hit okay, and it lets the threat actor get into the e-mail. A way to minimize this risk is to limit the number of MFA prompts that can occur within a period of time, which would mean that this MFA bombing would not be possible. And as always, employee awareness and training are absolutely key.

Kattman: Elise, as we close out today's episode, could you talk about the trends you see that are following us into 2023 and, quite possibly, beyond?

Elam: Of course. So, at the end of last year in 2022, we started seeing an increase in ransomware incidents. So, at the beginning of the year, we saw a slowdown and then it started ramping back up in the fall, and is not slowing down at all, and we think we're going to keep seeing that trend, at least for the time being. We're also seeing an increase in vendor incidents, especially related to secure file transfer software, which can have widespread impact to a large number of companies.

And if you want to learn more about the statistics and trends that we've talked about today and other interesting information related to incident response, please feel free to visit our online report at DSIR.bakerlaw.com.

Kattman: Thanks so much for joining us today, Elise.

Elam: Thanks so much, Amy.

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