Podcast Transcript

2022 DSIR Report Deeper Dive: An Introduction to the 2022 DSIR Report

Date: June 22, 2022

Guest: Ted Kobus, **Host:** Amy Kattman

Run Time: 10:04

For questions and comments contact:

Theodore J. Kobus III

Partner
New York
T: 1.212.271.1504 | tkobus@bakerlaw.com

Kattman: Ransomware, MFA, extortion, fraudulent fund transfer schemes. These topics and many others make up the key findings section of the 8th Annual Data Security Incident Response Report, informally known as the DSIR Report. Each year, the incident response attorneys within the Digital Assets and Data Management Group or DADM, provide statistics and analytics around the incidents they encountered the previous year in a report that is eagerly received by clients, vendors, media outlets and frankly anyone interested or tasked with their company's digital asset and risks.

This, our first in a series that will explore the 2022 DSIR Report, serves as an introduction and overview of the aggregated data from security incidents and insights, along with other relevant topics covering the entire data and technology life cycle. I'm Amy Kattman, and you're listening to BakerHosts.

Our guest today is Ted Kobus, Partner and Chair of the Digital Assets and Data Management Group. Welcome to the show, Ted.

Kobus: Oh, thanks for having me.

Kattman: To begin, can you tell us a little bit more about the history of the DSIR report? I understand this is the 8th issue.

Kobus: I know, I can't believe it. It is the 8th issue and it has evolved so much from our first report. The reason we started creating the report was really for marketing. We were handling so many matters in a variety of industries and we thought it was a great way to communicate our expertise. When the report was launched,

clients and the cybersecurity industry at large reacted really positively to it. The incident response team spends a lot of time on-site at clients, and I have managed matters where I was on-site for several months. While working with various clients, we started to see them bringing the report to meetings, making notes in the report and generally using it across the enterprise, not just the legal or IT groups.

It was really exciting to see, and as a result, in addition to the cybersecurity checklist and the 19 key findings we are providing in the report, we've expanded it to include content related to topics of interest such as blockchain and NFTs, litigation, privacy, advertising, as well as all of the data collected from the more than 1,000 incidents we help manage each year.

Kattman: So, that is great. Could you talk about some of the high-level takeaways from this year's report?

Kobus: There is so much to talk about when you look at the report. We worked on nearly 1,300 incidents last year, so there is, of course, a lot to discuss. It is not going to be a surprise to the audience that ransomware attacks continue at a high rate, and they remain the most impactful type of data security incident. However, clients are making investments in security enhancements and working on developing more robust business continuity practice, so there is good news here.

This makes companies more resilient and then less likely to choose to pay. That in turn drives down the average ransom payment amount. Still, threat actors continue to evolve tactics to increase extortion leverage, such as using publication countdown timers and contacting employees and customers directly to pressure the company to pay. E-crimes continued as well. There is a surge of wire fraud precipitated by gaining access to email accounts. Was some of this facilitated by information stolen in ransom attacks? Maybe. Whether it is or not, it is an issue that every company continues to battle, and we need to educate our workforce about it.

The recovery rate, however, increased in 2021. Funds involved in fraudulent fund transfer schemes last year were recovered 43% of the time, and that is up from 38% recovery rate that we saw in 2020. There is a very effective unit of the Secret Service that works on recovery funds. You just have to move quickly.

Kattman: So, that trend is going in the right direction.

Kobus: Absolutely.

Kattman: Can you tell us a little bit more about the trends you're seeing in litigation?

Kobus: Yeah. So, litigation continues to be a hot topic when talking about data security incidents. So, although we saw the number of lawsuits filed grow, we still only see a small percentage of matters resulting in litigation. So, what does that mean? Of the incidents included in the 2022 report, 23 resulted in one or more lawsuits. So, that is a pretty small percentage when you look at the overall

number of matters. Nineteen incidents involved Social Security numbers, five involved payment card data, 16 involved medical health information. So, that is really the information that is driving some of these lawsuits. Fifteen involved ransomware attacks, and four were related to incidents caused by vendors.

When you take a look at the size of the incident, eight lawsuits involved more than 1.2 million individuals, 11 involved more than 700,000, and three lawsuits involved fewer than 8,000 individuals. So, even though the big incidents are still generating lawsuits, we're seeing it more on the small side, too. Once a lawsuit is filed, on average, we see generally between two and five different complaints being filed. In larger matters that number can be much, much greater.

Kattman: Right. Going back two years, could you give us a snapshot of how the pandemic affected your clients' digital assets?

Kobus: Yeah. Being nimble was something I think we all learned from the pandemic in one way or another. And also, being nimble translated into better approaches to cybersecurity in my opinion. A company that is nimble in its security strategy is likely more resilient and better positioned to leverage the value of technology to support organizational goals and missions. Going remote had its challenges on so many levels, but in cybersecurity, employees were using devices that may not have been approved previously by the company, which always involves risk. Also, companies had to respond to that usage and implement protections to reduce the risk profile.

On top of that, they needed to deploy tools that provided better access and visibility into work devices being used at home. We have definitely seen companies improve their visibility into what is happening on devices across the network, however, a big game changer in the pandemic is that technology strategy and business continuity advantages are driving increased use of cloud assets. What does that mean? This also changes the risk landscape and makes additional security measures like asset management and access controls increasingly important.

Kattman: Understandably so. Ted, do you see any increase in cybercrime due to the war in Ukraine?

Kobus: Well, we have not seen an increase that we can directly attribute to the war in the Ukraine. We did see a drop in ransomware attacks towards the end of 2021 and into February 2022. For about four weeks, we didn't even get a call on our hotline over the weekend, and generally speaking we get one or two calls to our hotline every single weekend. That decrease, we're not sure about it, but it may have been because the threat actors, who happen to be mostly located in the Ukraine and Russia, were preoccupied with preparations for the war.

We're still watching this closely, and we continue to hear about threats to certain industries as a result of the war. The landscape in cybersecurity changes quickly, and the lesson we have learned is, do not let down your guard, and continue to

participate in threat information sharing activities, as well as ways to further secure your network.

Kattman: As one final question, Ted, is there anything else that you'd like to share with our listeners?

Kobus: Yes. A lot of work goes into creating this report, and we really thank our clients for having trust in us in helping them manage their incidents.

Going forward, we're going to have blog posts and other podcasts that dig deeper into the data, so you can understand how it varies between industries and what you can do to protect your company in a unique way. So, we're really excited about that.

Kattman: Thank you so much, Ted, for sharing this information.

Kobus: Thanks for having me. I really appreciate it.

Kattman: If you have any questions for Ted, his contact information is in the show notes. Be sure to stay tuned for our next episode of the 2022 DSIR Report, where we'll be discussing vendor incidents, which accounted for nearly 20% of the total incidents we handled last year.

As always, thanks for listening to BakerHosts.