Podcast Transcript

10th Anniversary Lookback: What a Long Strange Breach it's Been

Date: July 11, 2024

Guest: Eric Packel, **Host:** Amy Kattman

Run Time: 18:44

For questions and comments contact:

Eric Packel

Partner
Philadelphia
T: +1.215.564.3031 | epackel@bakerlaw.com

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

On today's episode, we're joined by Eric Packel, Partner in the Digital Assets and Data Management Practice Group, focusing on healthcare privacy and compliance at BakerHostetler. Eric will take us all the way back to 2014 and back again to look at the data breach landscape, how it's changed, where we are now, and what to look for in the future. Welcome to the show, Eric.

Packel: Happy to be here, Amy. Thank you for having me.

Kattman: Eric, I'd like to begin by you telling us what did data breaches look like 10 years ago?

Packel: So, that is an interesting question. So, I started at BakerHostetler roughly 10 years ago. And so, I've been here since the beginning of using the data for DSIR, and all of the DSIR reports and all the breaches that have happened over that time period. And I can tell you that 10 years ago, things were a lot different than they are today, particularly with the types of data breaches that we handled back then. So, if we were to get a data breach come in from a client, typically 10 years ago, we were looking at a lost laptop or a stolen laptop or some sort of mobile, small device, like a USB stick, maybe even hard drives, something lost or stolen

that had data on it and that was a typical matter that would come in. You'd be surprised at how many people, at least back then, maybe it is still happening, but they're not breaches and I'll tell you why soon, but back then, you'd be surprised at how many people would take a laptop home from work and on their way home from work, they'd stop at the mall, or they'd stop at a restaurant, or they'd stop at a bar, or they'd go to a party and they'd leave their laptop in the car, sometimes in the back seat, sometimes just the laptop, or maybe in some sort of case or luggage. And of course, they come out and their car is broken into and the bag and/or the laptop is gone and missing. And back then that was a major issue because as people didn't realize, I guess, but they learned over time, but they didn't know back then, just because you have a password protection, so anybody opens up a laptop, typically, they have to log in. That password protection when you're talking about computers and hard drives isn't necessarily going to stop someone from getting to the data. A lot of people didn't know that you could take out those hard drives. You can attach them to another device, and if you attach it as a secondary hard drive to another device, you just need to be logged in to that other device and you can see all the data on that hard drive.

So, those were the sorts of breaches that we had back then and they were difficult to deal with because a lot of times it wasn't known what data may have been saved locally on that stolen hard drive or missing hard drive or stolen laptop. And then you had to figure out well, what was there, what caused legal breach notification obligations? And unless they had a recent backup of that entire device, it was really difficult to determine that. And another thing that people didn't know is that back then, when people are using version of Microsoft Outlook that existed back then, now it is on the cloud with Office 365, but back then the version would typically save a file, a cached file onto the laptop, onto your local hard drive. So, then all of your emails would also be subject to discovery by the bad actor. So, over time, though, people learned how to deal with this. The big remedy for this, of course, was encryption. And as long as the device was encrypted when it was stolen, then we didn't have to worry about the data because in all the data breach laws, typically there is a safe harbor for encrypted data. And it took a while and maybe it took organizations having to pay a fine or to be subject to penalties for a data breach, took a regulatory investigation or took class action lawsuits, but eventually a lot of organizations learned you need to encrypt your mobile devices. You need to encrypt even USB sticks or just not allow them to be used. And you also need to not have just hard drives laying around that people can grab, particularly for backup tapes. We used to see a lot of lost backup tapes. Back in the old days they would transfer, physically, backup tapes to another location. Sometimes they would get lost in transit, or maybe they would just get tossed and thrown out by a cleaning crew. So, we had, those were the, most of the breaches that we were seeing in the early days. But now with encryption being so prevalent, it is rare that we have those types of lost or stolen devices as a data breach issue. So, that was what we were seeing 10 years ago to answer your question.

Kattman: Wow, we really have come a long way.

Packel: For sure. It is a totally different environment now. But I would say the good thing about all this is people learn that there are ways to avoid data breaches and encryption being one of them. And there was a lesson learned there and people really took it to heart because it is rare to see that now.

Kattman: Right. Well, Eric, how have phishing attacks in particular evolved?

Packel: So, back, again, 10 years ago when I first started at BakerHostetler, phishing attacks were happening then too. It wasn't just the lost or stolen devices, although that was a big part of it. But the phishing attacks that happened back then were different than what we see now in that it was less organized. It was more of a mass general attack on an organization, perhaps, or they're just spamming tons of phishing messages out generally, as opposed to targeting maybe individuals or even targeting organizations. They're just sending as many phishing e-mail messages out there, and I think that is how the name developed, right? They're just generally fishing for whatever they can catch, and if they were to get someone to respond to a phishing e-mail and give up their credentials so they could access their account, typically what happened back then is different than what we see now in that back then it was more about, well, they got into the account and maybe they'd use it just to send out more phishing messages, or they would rummage generally through the emails that they could access and see what was there that looked interesting. Maybe Social Security numbers or credit card information or health information, whatever they could generally find.

However, that's now evolved over time. So, the phishing attacks are more, I would say, specialized and targeted. They'll look for individuals that they think are a lucrative target, and sometimes will do that by going through websites of companies or LinkedIn or social media in general and seeing what they could find. And then they specifically send phishing emails to that individual or certain individuals at that level. We see this with hospitals, they might target physicians because they know physicians, they make a lot of money and they'll target them for maybe doing a redirect of their direct deposit by getting into their account, impersonating the physician and pretending that they want to change their direct deposit information. And then the next paycheck which they get once a month typically would go to the threat actor and they won't realize it maybe for several weeks. Because like I said, they get paid once a month, and by then the money is gone.

So, that is the difference in these phishing attacks. Another difference is they also evolve to really focus on, in addition to those direct deposit redirects I just mentioned, wire transfer fraud. So, a threat actor now will look at the emails to find out who is being paid, what vendor are they trying to pay here? And then they will target the finance department, the people who are dealing with sending large sums of money via wire to business partners or vendors, and then they'll access the account via phishing e-mail and they'll impersonate the CFO sometimes or some other finance person, and they'll get someone to send a wire transfer, not to the vendor or whoever they meant to send the money to, but to the threat actor. And that is really the big deal that we're seeing right now with

phishing attacks. It is, they're looking to monetize it quickly and they're looking to do that via those redirects of direct deposits in the wire transfer fraud.

One other thing we're seeing, which is very new and I don't know how far they're going to get with this, is using things like QR codes to get people to go to the website in the QR code, and that is a malicious website and it will, and it might download malware or it'll ask them for, to enter credentials and then the user has given up their account credentials. And another new method, in addition to emails, is text messages. So, via text message, they're also asking for similar information like in an e-mail and fooling users into providing their information. So, I would say generally overall the way phishing attacks have evolved is they're more sophisticated, they're more targeted, they're more concerned about directly and quickly monetizing as large sums of money as possible. So, that is where we are today with phishing emails.

Kattman: Well, thanks, Eric. Now what about ransomware attacks? How have they evolved over the last 10 years?

Packel: Well, what is interesting is when I first started here, ransomware attacks were almost non-existent. It was extremely rare. So, 10 years ago, what was that, 2014? I don't think we saw many ransomware attacks, if at all, until about 2017, 2018. And since then, they've taken off. And next to phishing attacks or I guess it is maybe a little bit more, we're seeing ransomware attacks a little bit more than phishing attacks, but those are the two big things that we're seeing these days. And ransomware attacks are clearly much more lucrative.

So, in the early days of ransomware attacks, to go over really what is different now between what we're seeing 10 years ago, is the amount of the ransom. So, initially we're seeing ransoms of tens of thousands of dollars, so maybe 20, 30, 40,000, something like that and of course, over the years that has gone way up and now it is not uncommon for the first demand in any ransom attack to be in excess of three, four, or $5 million. And we've seen even higher demands, and it is not uncommon for payments to be made, not just demand, but the payment to be made of over $1 million.

So, we're seeing more money demanded and paid in ransomware attacks. But another big difference is, in the old days of ransomware attacks, typically the attack would encrypt data, but they wouldn't necessarily take data. Now what we're seeing is almost every ransomware incident involves what we call data exfiltration. The data is being taken. So, it is double extortion. There is extortion to decrypt the data that's been encrypted by the ransomware variant, and there is also an extortion related to if you don't pay us, not only will you not get your data decrypted, we're going to publish all this data that we've taken from you and put it out on the dark web, or sell it or do whatever that they want to do with it. And so that is really the biggest change. And from a legal compliance standpoint, that is actually worse than the encryption, because with the encryption, sure it is an operational issue for any business if they can't get into their systems, but it is not necessarily a legal notice obligation because we don't necessarily know that they took or viewed or accessed anything other than just encrypting the data. But

now, once we get the ransomware note and we have a company communicate with threat actors to negotiate the ransom payment, they'll send a file tree list or listing of every file that they took, and typically it is multiple gigabytes, if not terabytes, of data, so there is a huge file list that then the victim has to go through and figure out what data was taken and then from that figure out, well, who needs to be notified? Is it employees? Is it customers? Is it patients? Is it someone else? Vendors' information? But that is really the biggest deal and really almost the biggest problem other than the operational downtime of any business that is suffering ransomware attack. In fact, we're also now seeing these days, compared to what we used to see, is what we call smash and grabs, where no data is encrypted, but they come in, they steal data, but they extort just for the data stolen because there is nothing encrypted, you're still up and running, but now you have the same issue of, well, they took data. It is illegal, and it is a compliance issue and also potentially a PR issue if they're going to publish it. So, those are the two biggest things that I think we're seeing now as far as the change in ransomware attacks with the amount of the ransom and that we're seeing definite data exfiltration in almost 100% of these incidents.

Kattman: Those are big stakes. So, we've talked a lot about the past 10 years and what we're seeing currently. Do you have any predictions for the next 10 years or 2034?

Packel: Wow, that sounds like a long time from now. But speaking of ransomware, though, I do expect, even though it sounds almost ridiculous to say that we're going to still have the same problem. I mean, the problem's been around for almost 10 years now, and I don't see it going away anytime soon. It is too lucrative with the millions of dollars in ransom payments that are being paid yearly basis worldwide, probably totaling over billions of dollars in ransom amounts that have been paid. And I don't think it is going to stop because most of the ransomware attackers are in countries where it is either supported by the government, or they turn a blind eye to it because they're not attacking local targets. They're Eastern European countries, maybe from China or North Korea, and they're attacking countries in the West. And unless that political aspect changes, I don't see ransomware going away anytime soon. It would also require a huge change in how networks are put together and how the Internet works. I also don't see that happening anytime soon. So, I think we're still going to be talking 10 years from now about ransomware incidents. What can we do to stop them? The attackers are going to evolve. The defenses will evolve with the attackers, but then the attackers will evolve again. So, I think that'll be here.

But another thing that may be a little bit new, and we're just starting to see it now, is AI, because there's already AI tools being used by many organizations and in some AI tools you can load information into it. It is not just asking questions. You're typing in information, or you're loading in information. If you load in sensitive data and then that data is accessed in an attack, then that is a data breach, potentially. So, I could see more and more of the use of AI potentially leading to attacks involving whatever AI tools that is being used at the time.

And on the public ChatGPT and things like that that is out there now, when that first started, and maybe it is still happening a little bit, but I haven't seen it that much lately, there were employees of certain organizations that didn't realize that they're putting information from the organization out basically on a public server when they're using publicly available ChatGPT or publicly available AI tools. So, we had to go through some data incidents, potential data incidents, where they were looking at whether it was a data breach when they found out an employee had loaded sensitive information onto one of those tools.

So, I think we're going to see a little bit more of that as the years go on and certainly in 2034, and who else, what else could there be in 2034? It is hard to predict the future, but I think we're certainly going to still need cybersecurity lawyers and we're going to have maybe even a bigger cybersecurity group than we now have at BakerHostetler still dealing with various data breach incidents.

Kattman: Well, Eric, thank you for this interesting and valuable conversation.

Packel: Oh, happy to go through it with you. And it is what I do every day. So, I enjoy talking about it.

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