Nota Bene Podcast Ep. 130

The New Global Business of Cyber Attack, from Ransomware to a Now-Ubiquitous State of Breach with Kari Rollins

Thank you for downloading this transcript.

Listen to the replay released June 16, 2021 here: www.notabenepodcast.global

Cyberattacks have become big business, from the standpoint of both the attackers, and attorneys pursuing liability compensation from corporate attack victims. Threat actors range well beyond hacker cults of old, now including sophisticated state actors, large businesses organized for the very purpose of cyber breach and theft, and complex threat networks that aggregate information formerly treated as innocuous. Ransomware is changing the state of cyber insurance, and both National and State regulations across the globe are entering the field to govern the conduct of business victims in this climate, both in terms of ransom payments themselves, and subsequent obligations to persons whose information goes out the pipes. Breaches, in short, are now a ubiquitous part of the multinational business landscape, and failing to test system vulnerability can present existential risk to any global business organization. We're joined by attorney and cybersecurity expert Kari Rollins to discuss what companies can, and in some cases must, do to prepare for a potential cyberattack.

This episode is a replay of Episode 114 which originally aired on February 23, 2021.

Guest:

Kari M. Rollins is a partner in the Intellectual Property Practice Group and an Office Managing Partner of the Sheppard Mullin New York office. Kari focuses on data privacy and data security, and complex commercial litigation matters. She has successfully represented clients in the financial services, audit and accounting, retail and fashion, food services, hospitality, manufacturing, and technology industries before state and federal courts, as well as in front of state attorneys general, federal regulators, and U.S. and international commercial arbitration forums.

Transcript:

Michael Cohen:

Welcome to Shepherd Mullin's Nota Bene, a weekly podcast for the C-suite, where we tackle the current national and international legal headlines affecting multinationals doing business without borders. I'm your host, Michael PA Cohen. Let's get started.

Michael Cohen:

Welcome to episode 130 of the Nota Bene Podcast. Thank you so much to all of our listeners in more than 100 nations around the planet. We so appreciate your continued participation in our ongoing conversations and your feedback. Please do keep it coming. It continues to help influence our programming. Given our current moment of cyber ransomware attacks, we thought we might replay episode 114 today, and that episode covers and canvases my conversation with New York's Kari Rollins about just this event. Kari not only presages a recurrent rash of ransomware attacks and warms companies large and small, domestic and multinational that it was coming, but she maps out how to safeguard against the event. And perhaps more importantly, precisely what to do step by step if a ransomware attack actually occurs.

Michael Cohen:

So given our current moment, I hope you all will enjoy this rebroadcast Kari’s prescient and profound counsel in this area. We will return to live programming again next week with Fatema Merchant in Washington DC, discussing the business climate, sanctions and autocracy in dealing with Russia, Russia, Russia. Until then, as always be well and enjoy this replay.

Michael Cohen:

My guest today is Kari Rollins. Kari obtained her undergraduate degree from Butler University in Indianapolis, Indiana. And for our multinational audience who may not be familiar with the United States education system, Butler is a wonderful liberal arts college and school perennially ranked number one, or among the top of the Midwest colleges in the United States, as well as nationally. And it's particularly well known for its Jordan College of the Arts.

Michael Cohen:

Some point after her undergraduate degree, Kari decided to obtain her Juris doctorate degree from DePaul University in Chicago, Illinois, right in the heart of Chicago, Illinois, where she graduated with high honors that are called summa cum laude, nearly the top of her class, if not the top of her class and Order of the Coif. What that means is that she did super well in her Juris doctorate program academically and demonstrated superior performance across the board.

Michael Cohen:

Kari is an intellectual property partner and an office managing partner in the firm's Manhattan Office. She focuses on data privacy and security. She is an avid speaker and publisher on the topic in the profession and she is ranked and recommended by just about everyone and everything. We will as usual attach our guests biography and a link to that biography to our show notes. If any of you are interested in exploring a little bit more about Kari and her background and experience. Kari, it is so wonderful to have you join me today on Nota Bene, thanks for coming on the podcast.

Kari Rollins:

Thank you for having me. I'm so excited to be here.

Michael Cohen:

Well, I'm really looking forward to our conversation. We haven't really addressed data privacy and cyber security in a number of months. I went back and checked. And what I think I took away from that lag in time is that this show will probably have nothing to do with prior shows, this is a field of conduct activity, law and regulation that is moving just about as fast as technology moves. And so it's long overdue and I'm really thrilled to have you on the show.

Michael Cohen:

Before we start to get into our conversation, I thought if you wouldn't mind, you might share a little bit with our listeners about your path to your current spot on the planet there in Manhattan and this particular field of practice that you have developed such an expertise in.

Kari Rollins:

Sure. Happy to do it. I came up through the ranks as a tried and true class action defense attorney or litigator. And about 12 years ago, one of our partners here, now at Sheppard Mullin, at the time she and I were at another firm. Liisa Thomas wanted to get a litigator's perspective on running a breached investigation, a data breach investigation. She thought it's good to have a litigator who can sort of see down the road how this breach may impact not only the company's business and notification obligations, but queries from regulatory authorities or private litigants if it results in such inquiries.

Kari Rollins:

So she thought best to have somebody have that lens now so that we can prepare the best offense down the road. And after doing that first data breach internal investigation, I was hooked. And that was about 12 years ago when the patchwork of laws wasn't what it is today. So I've had the benefit of watching as new laws are enacted across the states, learning more about the technology and really sort of immersing myself in all things data privacy, data breach, cyber security, and then now the cottage industry that has cropped out in data breach litigation. So it's been exciting to see how the world of data privacy has changed in the past dozen or so years when I first started focusing my career in this space.

Michael Cohen:

We'll talk about how it's changed in the last few months, if not few days. But that is a fascinating insight, meaning that you really were sort of on the risk assessment and dispute part of this field at its most nascent stage and have grown with it throughout its young history in law and regulation, but still not short history. I mean, we are talking about probably our second decade where this field has really developed and hope to talk a little bit about that development today. But share with me if you would how you wound up at Butler. I think it's one of the most interesting colleges in America and how you got from Butler to a field of law.

Kari Rollins:

Sure. So I went to Butler because I was a ballet dancer. I wanted to go to a college that had an incredible fine arts program. And Butler was ranked at the time, if not one or two in the nation for fine arts programs, in particular, the ballet program. And so I auditioned and made it and went to Butler and thoroughly enjoyed my time there dancing, but I was also exposed to new areas of education, which I was never exposed during high school. And I took a philosophy of law class and I really enjoyed it. And that maybe dance isn't where I want to continue to go down as a career path and switched majors in my sophomore year, continued dancing at Butler, actually danced on Butler's dance team for their basketball team, which is for those in listeners in the US, Butler has an incredible basketball team and it's very well known for its basketball. So that was really fun to be a part of Butler's basketball history and switched courses, and then found myself in Chicago and in law school and down the path I went. I haven't looked back.

Michael Cohen:

Is a fascinating background. Thanks so much for sharing it with us. And today's podcast will certainly benefit from your decisions along that way and really glad to have you with us today. So let's get right to it if we may. Just by way of staging, I think there've been a sea change of developments in this area or this field of business activity and disputes relating to computer system, cybersecurity and privacy and the area of breach.

Michael Cohen:

And what's really interesting to me about that sea change is it's sort of like the Atlantic hurricane season. It is a perennial annual sea change that seems to be increasing in its force and magnitude annually. The methods of cyberattacks change as frequently as hacker viruses, worms, and all of the other types of activity that lead one into a computer system illicitly and the motivations behind these attacks are as multi-phased today as they ever have been. And that motivation also seems to be expanding into areas that range from nationally sponsored state activities, to the full gamut of motivations that stem from the human mind, none of which are usually good.

Michael Cohen:

And it's not surprising in that climate to me that legal and regulatory landscapes shift so seismically, and so frequently as a result. We have seen a dramatically exploding cottage industry of legal professionals who now full time hunt and pursue data breaches. That didn't exist a year ago, two years ago, three years ago. It is now one of the strongest arms of an emerging bar of attorneys and attorneys in America play a massive role in corporate risk and liability. And that is a reality today that didn't exist a long ago and it may be described as relatively new.

Michael Cohen:

Insurance and claims amounts themselves have shifted dramatically, 20 millions of dollars in self-insurance or commercial insurance may not be sufficient to cover even a single claim. Hundreds of millions of dollars in those categories may not be enough anymore in America to cover a single claim. And single claims have exceeded those amounts with relative frequency, I should say, in our modern moment. So with this kind of two cents staging, which is always just my two cents Carry, I thought I'd throw it open to you really to say, hey, broadly, what do multinationals need to know about the most current developments on data breach in the US or I'll say computer breach more broadly in the US landscape?

Kari Rollins:

Sure, of course. I think with the sea change that you described, which is absolutely correct. There are really five truisms that have resulted that I think companies need to understand when they evaluate cyber security and the risk of a data incident and any fallout there from. So sort of the first truism is that data breaches today are ubiquitous. They are global, they are pervasive and they are all manner of shapes and sizes. They can range from massive crippling ransomware attacks like the new ransomware attack group, Egregor, that I've, I don't know if I got the honor of having dealt with one of or at least a couple of their very first attacks when they stepped on to the scene in late September of 2020. These are ransomware attacks where the demands are $40 million, $30 million, the likes of which the FBI had not previously seen.

Kari Rollins:

So these ubiquitous data breaches or data incidents could be a ransomware attack, it could be the exploit of a software vulnerability, like what we saw with the solar winds data incident, which I have also unfortunately had to handle or assist clients with. It could be as simple as a business email compromise when an employee clicks on that very thoughtfully crafted and socially engineered fishing email. And it could also be something as simple as a lost computer. So I think what companies have to understand is it may be the ransomware attack that they see, but it could also be something as small and as seemingly innocent as clicking on an email. And then you've then given the keys to the kingdom because of the access that the threat actors have to your computer and then your network.

Kari Rollins:

I think the other truism, and I'll sort of step into each of these first and then we can circle back with questions, is that you are a target. Regardless of your business, regardless of the type of business that you conduct, you are a target for a variety of reasons. If you have employees, you have information about people that is useful. If you have consumer facing websites that process payments, you have information that is useful. Even if you're a manufacturer, you have information that threat actors find useful because you have information about corporate customers, you have access to other vendors.

Kari Rollins:

And so the threat actors are working together at a remarkable rate today to exchange and share information. Think of it as a bit of a spider web. They continue to build out the circles of their web with aggregated pieces of information that they collect from different data incidents. So just because your company isn't collecting payment card information about a consumer, your company may have information about a corporate customer that the threat actors can then pair with email addresses or other information about say the CFO of that corporate customer socially and engineer an email to them that looks legitimate and try to defraud them out of a wire transfer of hundreds of thousands to millions of dollars.

Kari Rollins:

So these threat actors are sharing information with each other, they're not operating in a silo and they're aggregating it in order to construct very thoughtful attacks. So that is also a truism. You are a target. I think the other truism is that the regulatory landscape that we talked about is a global patchwork and it is ever changing. And unfortunately it's also becoming increasingly punitive. So you have instances where the obligations to notify even an incident that may not impact payment card information, something that impacts usernames and passwords or other non, what we would consider sensitive information.

Kari Rollins:

You may still have an obligation to notify consumers and each state in the US and foreign jurisdictions have their own requirements for notification. So understanding what your obligations are is a monumental task. You have to understand the laws and you have to adhere to the timetables implemented by those laws.

Kari Rollins:

Obviously coming from the ubiquity of a data breach is the fact that you're also being placed under greater scrutiny. So a company's cybersecurity practices are being scrutinized even more than they ever were. The Biden administration has placed cybersecurity as a priority. State regulatory authorities have placed cybersecurity as a priority in New York in particular, as well as obviously, California, Florida now too. And that scrutiny, the scrutiny that's placed is viewed through a lens using 2020 hindsight, which is never great for a company.

Kari Rollins:

You can have a data incident and of course the regulatory authority or the private litigant standing on the other side of it are going to go, well, you should have done this, you should have done that. You could have prevented this data breach if you did X. That's not always true. And in fact, I find it's very rarely true. But now today, if you have a data incident and it becomes public, you can fairly well assume that you're going to have a regulatory inquiry or litigation that's going to arise from it. And then that litigation is going to test what you did to protect the information, no matter how harmful or valuable you believe that information to be.

Kari Rollins:

Is it simply just purchase history? Is it not even sensitive, personal information? Maybe it's names, email addresses, addresses, and phone numbers that were impacted. How did you protect that information? The fifth and sort of final truism that I think complicates all four of the other factors is that we are living in a world where consumers and individuals demand what I like to call transparent privacy.

Kari Rollins:

Everybody wants their information to be private. They want it to be protected. They expect it to be protected, but at the same time, they want everything in the open. They want all of their devices connected. They want access now, they want access through easier non interpersonal electronic means. And with the interconnectivity of devices and the transparency demanded, it's harder for companies to understand and evaluate how best to protect the information that their clients, consumers, customers, and employees are demanding be interconnected and transparent. Sort of the big construct over which I look at all of these items. And that's all to say that I think cybersecurity preparedness looking at the lens of how you're going to be tested is sort of the key here.

Michael Cohen:

I love that framework that you have laid out for us, the outset of the discussion. I mean, those are brilliant and digestible and stark flagpoles for us to have a bit of a conversation around. And let me start with the first you mentioned, the ubiquitous nature of attacks and breaches in the current world. I once had the great privilege and opportunity to work with one of the most brilliant minds in computer science of at least my generation, well, not my generation, he's from a very former generation, but I'll just say period.

Michael Cohen:

In computer science history and mathematics, I'll just say period, a guy named Dr. Paul Schneck, who I'm sure would not mind me mentioning his name on the air. And I remember sitting with Paul and a very sophisticated computer science company in the business of computer security defense. And we were talking to third party who was in front of us. And the third party was insistent that they had never been breached.

Michael Cohen:

And just remember Paul looking at the guy and smiling and I was waiting for it because I'd heard him say it before, and you probably know what's coming, but his comment was quite simple. How do you know, how do you know right now that you haven't been breached? You have no idea what you don't know and breaches aren't something where you opened the fire door and the alarm goes off. I mean, the whole purpose of a breach is for the alarm not to go off. The entire design of a breach is designed to be undetected and so many companies, so many sophisticated companies, companies in the business of computer systems and computer science themselves, I think don't really focus often enough on one simple point.

Michael Cohen:

So what do you say to those folks? What do you say to kind of the folks out there in the current environment who may be two years ago said, or even last month said, you know what, got pretty sophisticated systems. We're kind of a hard nut to crack and everything seems to be working. We'll deal with something when it happens, but otherwise, we're going to kind of bury our head in the sand approach. We'd rather not know what we don't want to know, and when it becomes something we should know, we'll deal with it. Because I would imagine that's fairly pervasive in the multinational environment and any domestic environment really.

Kari Rollins:

Sure. So I think what's important is regardless of the security measures you have in place, you have to account for the human aspects, human error. I saw a statistic that data breaches today, 52% of data breaches today are caused by human error. And that could be as I mentioned, clicking innocently or unwittingly on a phishing email that is so carefully crafted as to look real, that you actually believe it to be real. And it's not just folks without information technology backgrounds that are clicking on these emails unwittingly. I have seen on several occasions, just in the past few months, information technology, information security employees who have been the ones to click on these emails that have given the bad actors access into the network. And because these IT or IS folks have administrative privileges, the threat actors gain access into the environment and quickly have administrative rights that they can elevate and then push malware through the networks.

Kari Rollins:

So you could have all the great security measures in the world, but if you're not taking steps to train your employees, all employees to detect phishing emails, to advise them on best cybersecurity hygiene and health practices, then you're really not setting your company up to mitigate the risk, sort of reasonably mitigate the risk of data incidents.

Kari Rollins:

Separate and apart from that to your putting your head in the standpoint, it's really important to test your data security compliance and how your tools are operating. I can't tell you how many cases I defend where the issue on the table is that there may have been a practice in place that wasn't followed, or there may have been a document that said we're going to do X because it was a very lofty goal, cybersecurity goal. And one that probably wasn't necessary, it was just a really lofty cybersecurity goal, but X is never achieved.

Kari Rollins:

So then you have a document stating out there, we love to do X, this is a great cybersecurity tool. And then you never implement X. Well, then the plaintiff's counsel come and say, well, look, they knew exactly what they should have done, and they never implemented X. So testing your cybersecurity compliance program and auditing your systems, doing vulnerability tests, doing penetration tests is a critical component of any cybersecurity preparedness. You can have the greatest tools in the world, but if you're not testing them to see if they're functioning appropriately or you're not testing the controls around them, then they're going to be irrelevant if you have a data incident that has exploited a vulnerability in those tools or a gap in that coverage.

Kari Rollins:

Those are the instances that are going to be heavily scrutinized with 2020 hindsight by private litigants and regulatory authorities. And even more importantly, you insure. I see today now because ransomware attacks are really being deployed at breakneck speed and because ransom payments are being paid by companies that can't or didn't have backup systems or their backup systems were encrypted. Insurers are starting to more heavily scrutinized the security posture of their insurance, and they are sending cyber renewal policy questionnaires that are pages long asking them or asking the insured what their cyber security posture is, so that they can assess risk. How risky is it that if this company has a data incident, it's going to rise the level of a data breach that requires notification and has fall out litigation, and they're going to adjust their premiums and the coverage that the insured needs given their risk assessment.

Kari Rollins:

Or alternatively, if a company fills out a cyber policy that says we're doing X, Y, and Z, and then you have a data incident, and it shows that you were only doing X and Y, the insurer's going to say, well, you misrepresented to me on your application, or even in a post application, email exchange, what you were doing to secure your networks. And because you didn't have Z deployed, you created a greater risk of compromise or greater risk to your environment and you've misrepresented that health and wellness to us and you've now lost coverage for this data incident. So I would say having great security tools in place is really important. That's a great first step, but training and auditing and compliance is critical.

Michael Cohen:

Yeah. Sort of sounds in some respects, practically or legally, and maybe both Kari, that training and system vulnerability, I'll call it testing, which can include penetration testing and all kinds of other types of computer science, white hacking challenges to kind of self-scrutinize your own system. That's where people, I think really put their head in the sand. They don't want to do that. They actually don't want to find out their own vulnerabilities because they feel well once they find that out, then they have to fix them.

Michael Cohen:

And yes, that is probably right. But you also have to find that out now, I think from what you're saying. Because if you don't do that, what I just heard you say is that those are become minimum legal standards in some sense. So if you have a data breach and you haven't done those things, you're pretty much out of luck, but putting your head in the sand may no longer be a legal option. What's your reaction to that? Am I anywhere close to the mark?

Kari Rollins:

No, I think that's exactly right. Ignorance is not bliss when it comes to cybersecurity. And depending on the industry within which you work, where you operate, you may have audit and compliance obligations. For example, companies who are subject to the New York Department of Financial Services regs, cybersecurity regs have audit and attestation compliance obligations on an annual basis. And that's because the New York Department of Financial Services evaluated properly that there's risk to financial institutions to insurers when it comes to cyber security and they wanted to ensure that the entities over which they had regulatory authority were taking appropriate steps to address cybersecurity or information security.

Kari Rollins:

So you may actually have an audit and compliance obligation if you were in a specially regulated industry, but separate and apart, even if you're not, that is certainly going to be a test of reasonableness, which is really the standard when you come to litigation, reasonableness of your cyber security program. The question is always going to be, did you have reasonable security standards employer? Were you following reasonable cyber security standards?

Kari Rollins:

Not surprisingly, what a reasonable cybersecurity standard is, is not defined. There are industry standards that individuals or private litigants will look to test whether you have reasonable measures, standards like NIST are often referred to if you are processing payments than standards issued by the payment card industry. The PCI DSS standards are certainly a test as well. But again, it's going to be a matter of reasonableness. So when you're putting together your security program, you really need to think sadly with the end in mind. You need to think, how am I going to be able to provide a really strong security story? That's what I tell all of my clients, what is our security story here?

Kari Rollins:

So even when we have a data incident and I'm sort of enmeshed with my client, directing the incident response, I'm also asking questions if I don't already know this, and haven't been involved from the get go of what's our security posture? What's our security story? Because I can guarantee if we issue regulatory notification, if the data incident rises to the level of a breach that requires notification, we are going to have follow-up questions from state regulators, or if it's a global notification, foreign authorities on what our security posture looked like, what measures did you have in place to prevent this data incident or to mitigate the risk of this data incident?

Kari Rollins:

And you want to present a good security story to those regulators. You don't want to just answer the question and ask, you want to be able to give it to them in a really nice narrative that hopefully ends the follow-up questions right then and there. But I think that's what you need to think about when you're putting together sort of your written information security plan, your cybersecurity program is, do I feel comfortable sharing this with the world, or is it going to look like I scrimped and saved here to the detriment of maybe the individuals whose information were impacted?

Michael Cohen:

Super salient counsel. Thanks so much for sharing those thoughts with us. My next question for you relates to the spider web metaphor, I suppose, that you shared with me. And that really did strike a chord. I'm an old math major so anything that has some sort of natural trigonometry to it, because trigonometry explains so much in nature. It's just so perfect. It's indescribable. And a spider web is one of those things that is just a mathematical system at work. And the fact that it comes from an eight legged creature that can be the size of a thumbnail is just probably one of the most largest engineering marvels in human observation.

Michael Cohen:

But I thought that that web analogy really made a lot of sense, meaning, because there were a couple of things you said with it, as I heard you Kari. Number one, data breaches are now ubiquitous to the threat actors, I'll call them hackers because I'm kind of old school, are working together. This is not kind of a novel thing anymore. This has become a big business and a global business. And many of these networks of hackers are just full on companies themselves in the business of doing this. And they're doing it from remote locations all over the planet. They could be anywhere and not even together. And that they're sharing the information now in order to use it in some way that is aggregating bits and pieces of data as that web grows.

Michael Cohen:

So almost any kind of data becomes important in how it fits into building that web out. That's a pretty scary environment. Particularly as modern data science continues to achieve its own exponential breakthroughs, according to same kind of exponential growth that we've seen in semiconductor and other principles and laws and technology. And so that is making information of all sorts more valuable to anybody in an industry that's growing and in the business of hacking it. That seems to me to be a pretty scary environment. Did I put together those points correctly?

Kari Rollins:

Yes, absolutely. It's not just the case anymore that you will have a data incident by a single threat that occurs as a result of a single threat actor group. We are seeing it frequently now where you could have a data incident that has footprints of two threat actor groups having been involved. Maybe the first threat actor group is the one that used credentials that they had stolen or purchased from another threat actor group in order to break into your network. And then maybe it was the second threat actor group that then deploy the encryption malware and how the system is for ransom, or maybe it's the second threat actor group that came in and stole personal information. Acquired the initial access from the first threat actor group and stole personal information from the system to further exploit. So we are seeing them work together and we're seeing them aggregate information.

Kari Rollins:

And we're also, it used to be that this information was being sold on the dark web and that was the purpose of it. The purpose of a data breach was to acquire information that could be sold by the bad actors. We're not seeing that as the only use for the information today. We're also seeing information released as punitive reaction to a failure to pay ransom or just to embarrass or otherwise, just to put information out there that the threat actors have deemed depending on who the threat actor is, if it's a nation state that threat actors have deemed important to share with the world.

Kari Rollins:

So we're seeing information being released rather than just simply sold on the dark web. And it is a scary proposition, it's important too in the context of injury. Not every data incident is going to result in injury to the individual whose information has been stolen. And that's a big issue that's tested in litigation today. It's always a matter of how the individual's been injured. And with the way that companies now react to data incidents to provide credit monitoring, to provide threat detection and prevention services to impacted individuals, where the credit card company is reimbursed for fraud so quickly. The question of injury is a big one. Has there been injury to the individual if their information has been stolen? And so that is always a big question on the forefront of all of our litigation today, no matter how the information is collected or aggregated or what the information may be.

Michael Cohen:

Your breadth of intuition and experience in this arena is nothing short of amazing. And certainly reflects at least to me, somebody who has lived this field and not just studied it, but lived it. It's so much fun to get to talk with somebody who has lived some field like you have Kari. You've mentioned ransomware a couple of times, if not more. And I wondered if you might just spend a moment with our multinational audience on that topic, because it is certainly one that every company, multinational or not, frankly, faces every day that the 24 hour clock ticks forward to the next day.

Michael Cohen:

There isn't a day that goes by where ransomware isn't a possibility. It doesn't matter who you are, if somebody can get in, freeze your systems and freeze your business until you pay them, that is the ultimate form of Buccaneer piracy. That would make anybody living an 18th century life in the Caribbean thirsty for.

Michael Cohen:

So I would imagine in a 21st century environment where you can be an anonymous pirate and not have to work very hard for that kind of ransom, that's a pretty big area of activity. And it is one where we have seen growing and growing incidents reported in the press. I mean, it almost happens every day it seems. So may I stop talking and let me just hear if you might share with our listeners what they might need to know in this area, because this is an area that just is plain old commercial, affects their insurance, affects their livelihood, affects their ability to operate in any moment, given the fact that crippling those operations is the object to obtain the ransom. So I hoped you might share a little bit about modern developments there.

Kari Rollins:

Sure. So I think being prepared for a ransomware event is really important. And I think sort of the two best pieces of preparedness apart from having an incident response plan that you've tested is backup systems. Having backups that you know that you can restore quickly if your primary systems are encrypted and having them segregated in a way that would avoid, if your primary systems are encrypted, lateral movement to those backup systems.

Kari Rollins:

So the backups are really key because if you don't have viable backups or if your backups have been encrypted, then the necessity to pay the ransom may increase because you don't want to be out of business for two weeks, losing millions and millions of dollars a day while you work to rebuild your systems, systems that you hopefully could have restored from your backup in a matter of 48 hours, two days.

Kari Rollins:

So if you are crippled and your backups are crippled, then you may have to pay the ransom to the ransom attackers in order to obtain the decryption key from them and get access back to your systems. And even then, once you've paid them, you're not guaranteed that the decryption key is going to work though there's this sort of new nuanced evolution of ransomware negotiations that has occurred where you have different stages in ransomware negotiations. And you can ask for evidence of decryption from the threat actor group, but it doesn't mean that the decryption is going to work or that it's going to be fast.

Kari Rollins:

So it can take time even after you've paid the ransom and more money. So you could be out of business for a week, two weeks, three weeks, even after you've paid the ransom and obtained the decryption key, because it may take you time to apply that decryption key to each system to decrypt it and then bring it back online.

Kari Rollins:

So it's a very expensive proposition if your backup systems are encrypted or non-existent, or have been destroyed or otherwise deleted. So I would say backup hygiene is really critical in preparing for a ransomware event. If you do get hit with ransomware, don't panic. Though, I know it's very hard not to do. And have an alternative plan if your email is itself encrypted. Having a separate mode of communication that your incident response team can get on really quickly to triage and respond and know who the investigators are going to be that you're going to use to help investigate the ransomware event.

Kari Rollins:

Know who your friends with investigators are going to be, know who your counsel is going to be to help you walk you through that incident response, know who your crisis communications team is going to be in the event the ransom attack becomes public. And then also know your insurance, insurance is critical, a critical component. There was an article two days ago where there's a question by New York regulatory authorities over, should insurers really be permitting or encouraging their insureds to pay ransom amounts at the rates at which those ransom amounts are being paid both in dollar amount and velocity?

Kari Rollins:

Because the question is, is that just perpetuating future ransomware attacks? Is that just encouraging more ransomware attacks? I don't know that the threat actors think that way. I don't think they are necessarily going out and holding systems for ransom because they know a company has insurance that will cover it. They're just doing it. So I don't know if insurers changed the requisites needed to pay a ransom amount under the policy, if that will affect the rate at which ransom is being deployed.

Michael Cohen:

No. They may just cast a wider net. I mean, they're fishing in essence. You have to assume that insurance is the motivator. And I think the point you're making there is that there's no evidence that that's the case. They could be casting wide nets and see who has money to pay. And by the way, a lot of companies, I think try to self-insure in this arena because it can be very difficult to get commercial insurance at certain levels. And it's becoming more difficult given the risk is going up and there's only so much you can get. And by the time you're into re-insurance layers, you're into a dispute because the re-insurance companies never pay without some dispute resolution after you're fronting. So, yeah, that's a really interesting point you raise Kari, which is, I like your question. Before you can answer that, you really have to establish that insurers are the motivation for the attack. And what you're saying is I don't see that.

Kari Rollins:

And I mean, again, I understand from the insurance perspective, the pain that they are feeling. They are paying out claims at breakneck speed these days. And that's why, again, more scrutiny is being placed on the insurance with respect to their cyber security, hygiene and preparedness. And also more scrutiny is being placed on them with respect to how they respond to an incident, how they respond to a ransomware event, whether they pay the ransom or not and why? Why did you need to pay, did you not have backups? Did you say you had backups in your application, in your renewal? And were those backups not sufficient? And that all goes to some proof of loss there too. So again, there are a number of factors that will determine whether an entity wants to or needs to pay ransom.

Kari Rollins:

And then compounding that is the fact that if the threat actor organization that perpetuated the ransomware is affiliated with a terrorist country or terrorist area or regime, and then they may be on the OFAC list, which would then preclude a company, even if it needed to, even if it didn't have viable backups and had to restore, had to pay the ransom, they would be precluded from paying that ransom or they could, I guess, pay it and then be subject to significant signs.

Kari Rollins:

Though, if there are payments occurring via Bitcoin, which is how most of these pit ransom payments occur, and the FBI sees massive dollars in Bitcoin being paid to purses or wallets known to be associated or areas geographically located with sort of OFAC territories, OFAC listed territories, then they could step in and actually stop that payment too, the payment may not go through. So there are a number of considerations when you're dealing with ransomware that will dictate whether you can pay the ransom or not, even if you need to.

Michael Cohen:

Can we just pause. I'm sorry, but I think that's worth pausing on. I mean, I think I just heard you say that you could be attacked and held hostage in a ransomware situation and the United States Federal Bureau of Investigations, OFAC regulations, or I should say the nation's OFAC regulations enforced by the FBI and other agencies would literally prevent you from paying the ransom and decrypting and unfreezing your systems and your business injury would just go on until you could resolve the issue or obtained goodwill from some folks in countries on that list, which is highly unlikely. So is that what I just heard you say?

Kari Rollins:

Again, the transaction could be flagged. The transaction could be flagged and the account frozen, depending on the method again, through which you're making the payment, which is often the case when we're dealing with a ransom payment where we work with the FBI, just to say, hey, look, this is a non OFAC threat entity, but we're going to have to make this payment. We're just letting you know so it doesn't get flagged and frozen, because we have a certain amount of time within which to make the payments.

Kari Rollins:

So that's often a phase of ransom response that has to occur in order to make a payment since you're making them through Bitcoin or other cryptocurrencies. And if they're being paid in high dollar value amounts to territories that are not otherwise known, they can often occur and appear very suspicious to those that are watching.

Michael Cohen:

Well, I'm just so fascinated by the 21st century world. Hearing all of this, as you talk about the cryptocurrency payments, I can see a whole bunch of people who get excited that that's occurring in cryptocurrency.

Kari Rollins:

Yeah. No. I had an incident where we had to make a payment via Bitcoin and it takes quite a while to actually make all these different transactions. And it was a Saturday night and I was up with the entity that we were using to make the payment on behalf of their client. And I'm sort of every hour on the hour, 12:00 AM, 1:00 AM, 2:00 AM, 3:00 AM, 4:00 AM looking at my computer screen, watching the Bitcoin payments go out in these trenches and sort of approving them.

Kari Rollins:

So it was a fascinating process, but if you do have to make payment, there are a lot of factors to consider when you make it. It's not just as easy as writing the bad actors check by any means. For the listeners out there too, if you do get attacked and you are considering making the ransom payment, you should use or you should contact your counsel or use a third party intermediary because engaging with the threat actors and paying it could open you up to a secondary attack.

Kari Rollins:

So I've often seen it when we were making the payment, the entity that we used to make the payment started itself experiencing attacks because the threat actor world or the bad actor world saw these payments going out and thought, hmm, they're making some ransom payments, we're going to try and attack their systems. Do you want to use a third party or go through a third party to make these payments that can be made in a secure, safe fashion that protects you from secondary attack when you're making that payment?

Michael Cohen:

Your life is like a, well, I would say a spy novel, but it's not like a spy novel because if you read a spy novel, you would say, no it's way beyond that at this point. Kari Rollins, I have had you for probably more than the time you have allotted for the show. But I did want to take a stab at asking you just before we wind up, if there's anything else you think we ought to hit right now, I would love it if you would come back on our show on a more regular basis to keep benchmarking us and pulling us along a field of conduct and a field of law and regulation that is changing monthly, is probably a really fair way to put it. So two things, will you come back on the show and a second wind up, is there anything we ought to hit today that we may have missed?

Kari Rollins:

Sure. I would love to come back on the show. I've thoroughly enjoyed this and this topic is really expansive. And it's just something that is obviously near and dear to my heart and I live and breathe it and love it. And I think the only thing that I would say, and in concluding our conversation is just two companies contemplating their cybersecurity programs. It may appear expensive and often the question becomes, gosh, do we really need to secure X, Y, and Z? What's the benefit here? Is it going to be a loss leader? I think the lens through which you're going to be tested is always going to be 2020. So I think it's really important that companies when they put together a cybersecurity program, they think about, again, are you comfortable telling your cyber security story to the Attorney General, to a private litigant in a court setting? Do you feel like you can support that story and that it's been tested? Because that's really where you're going to be scrutinized.

Kari Rollins:

And if you've avoided spending money on cyber security because you didn't deem it was important, you may or may not have needed to do that, but that's always going to be questioned certainly by private litigants and litigation and by regulatory authorities. So I'll sort of just close on saying that, which is, be thoughtful, be deliberate, and think about if you had to present it in a public forum, you'd feel comfortable about that cyber security story that you're telling

Michael Cohen:

Such insight. Thank you so much Kari Rollins for being on the Nota Bene Podcast.

Kari Rollins:

Thank you.

Michael Cohen:

Well, that's it for this week folks. As always, thank you so much for listening.

* * *

Contact Information:

Kari Rollins' web bio: Kari Rollins: Sheppard Mullin

Thank you for listening! Don't forget to FOLLOW the show to receive every new episode delivered straight to your podcast player every week.

If you enjoyed this episode, please help us get the word out about this podcast. Rate and Review this show in Apple Podcasts, Amazon Music, Stitcher Radio, Google Podcasts, or Spotify. It helps other listeners find this show.

Be sure to connect with us and reach out with any questions/concerns:
LinkedIn
Facebook
Twitter
Sheppard Mullin website

This podcast is for informational and educational purposes only. It is not to be construed as legal advice specific to your circumstances. If you need help with any legal matter, be sure to consult with an attorney regarding your specific needs.