FOLEY

FOLEY & LARDNER LLP

Health Care Law Today Podcast
Episode 13: "Tune Up" Your Cybersecurity Program: A Perspective on Why Now

On the heels of recent significant Office for Civil Rights (OCR) breach settlements—one related to the Protected Health Information of 6 million individuals, and two allegations related to systemic noncompliance with HIPAA rules and a potential violation of HIPAA affecting over 10.4 million individuals—Foley Partner Jennifer Rathburn talks with Brian Resler a Vice President for Engagement for Stroz Friedberg, an Aon company, to discuss practical and approachable steps you need to take to tweak your cybersecurity program to be better prepared for any potential attacks.

Jennifer Rathburn focuses her practice on helping clients prepare for and respond to data breaches, as well as complying with HIPAA, 42 CFR Part 2, GDPR, GLBA, FERPA, and other federal and state privacy laws. She is also co-founder of the Midwest Cyber Security Alliance, a nonprofit, nonpartisan collaboration of stakeholders focused on promoting awareness of hot cybersecurity and privacy issues as well as advocating for more effective solutions.

Brian Resler manages teams assisting clients in responding to data breach and cybersecurity incidents, developing and implementing information security programs, and conducting digital forensics for litigation. Prior to Stroz Friedberg, Brian spent about 25 years as a State and Federal Prosecutor, most recently as a litigation supervisor for the U.S. Department of Justice Computer Crime and Intellectual Property Section, supervising and advising on cyber and intellectual property prosecutions around the country.

Please note that the interview copy below is not verbatim. We do our best to provide you with a summary of what is covered during the show. Thank you for your consideration, and enjoy the show!

Jen Rathburn

Thanks Judy. Hi, my name is Jen Rathburn and I'm a partner at Foley & Lardner.

In light of the increase in ransomware and new security vulnerabilities from working from home, as well as recent publicized cases about cyberattacks related to the attempted theft of COVID-19 vaccines and studies, we really wanted to do this podcast to help you focus on what needs to be done to protect your organization. With me today, I have Brian Resler, the Vice President for Engagement at Stroz Friedberg, to discuss some practical steps to tune up your cybersecurity program. Brian, welcome!

Brian Resler

Thanks, Jen.

Jen Rathburn

I think where we first want to start out is just, why now? Why now should we do a podcast that's focused on health care? I teed it up a little bit because, as you and I both know, we've seen a rampant increase of cyberattacks, in particular focusing on ransomware, but I would love to just get your general overview thoughts. Really, why now?

Brian Resler

There's a couple of things I'd like to highlight, but specifically focusing on health care, I think in any capacity, health care is always a target for cybercrime, regardless of what's going on in the outside world, and there's a myriad of reasons for that. I'd like to highlight two that I think are particularly relevant. One is, from a threat actor standpoint; there's a perception that there's a significant amount of financial assets involved in the health care industry, and that's true regardless of the actual size of that business, its role, and any assets that it has. So whether you're a major hospital, research center, or a drug or equipment manufacturer, or perhaps just a small local clinic or nonprofit to aid professionals, the belief is, there's a significant amount of money passing through. And while threat actors often act to cause disruption and other sorts of mayhem, predominantly what they're doing this for, is for a means of earning a living. Essentially, it's their full-time job and they're trying to earn money, so they target that industry and the kinds of industries that will bring them the most bang for the buck, if you will.

Jen Rathburn

That makes sense.

Brian Resler

And there's a perception as well that urgency is involved with health care, and this is funny because it plays both on public perception and business perception to the benefit and to the leverage of their threat actors. From a threat actor standpoint, they recognize that the public needs health care and it's an urgent need, and when you have to have it, you need

to have it. As well, there's always the business need, that a business needs to be operable at any given moment, but particularly for health care, it's not the kind of business that can afford to take, perhaps, two weeks of downtime. No business, certainly in any circumstance, wants to have that, but for health care, the understanding is you have to be able to provide that need as soon as the need presents itself. That gives the threat actor leverage in a variety of attacks.

For example, focusing on ransomware matters, if a hospital's systems are encrypted and they can't provide care for their patients, that is a significant amount of leverage for a threat actor to try to extort money from that hospital who otherwise, in a different industry, might be able to spend a week or two rebuilding their systems and avoid paying that ransom.

Jen Rathburn

On that note, we have seen many ransomware attacks upon hospitals, health systems, providers, et cetera, and a few years back the Office for Civil Rights did release some guidance related to how to prepare for and respond to ransomware attacks as well as how you do the breach analysis. So, ransomware has been something that has been around for several years, but as you and I both know, we have certainly seen an uptick.

Brian Resler

Absolutely, and one of the problems with the uptick is the current pandemic. There's a number of factors that I think any business needs to pay attention to during this time, but particularly health care is especially vulnerable. First, I'd focused on the fact that many more employees are working remotely than ever before, and that is a problem for a couple levels. One, it gives the threat actors a lot more surface area to attack. When you have your employees working in one building together, the IT manager has to just worry about the people in that building and can more closely monitor and enforce network policies.

When we have to transition to teleworking, and if your business is not prepared to do that and you've had to make adjustments, oftentimes there're shortcuts, there's things overlooked. People are allowed more access privileges than they should have, and that can lead to a compromise of those accounts and giving a threat actor a leg up on the system. For example, giving them administrative privileges when they shouldn't have it. So that's one stress.

There's also increased financial strains, and unfortunately too much for businesses going under and not being able to sustain or transition their business during the pandemic. But even in a best case scenario, and especially for businesses involved in health care, there's reduced revenue, and there's increased operating costs to adjust to safety concerns. When do you meet patients? How do you treat them? If it's just internal employees, can they all work in one location? What steps do you have to take to keep everybody safe?

Even if you've done all that, you have to consider your third party vendors and suppliers. What businesses do you engage with and what steps are they taking? And it may be that, while your system is pretty safe and secure, the people you deal with are struggling and they're having problems with their systems. So that also creates a further stress on your own business and your own ability to operate safely in this environment.

Finally, I would note that the increase in cybercrime that we've seen lately has been largely due to the pandemic. There's been a number of statements issued by the FBI and other law enforcement entities warning businesses that attacks such as business email compromise and fraud are on the rise. Ransomware attacks are on the rise, and we're even finding increases in attempted theft of confidential or trade secret information.

I would like to highlight, if some of that is not clear enough, that just a few weeks ago, the Department of Justice issued a notification that on July 21, 2020, they issued charges against two Chinese hackers with the Ministry of State Security. This was a global campaign by the Chinese government to target intellectual property and confidential business information, and pointedly, including COVID-19 vaccination research and testing. You can see that there's a lot going on due to the pandemic. Not only are people more vulnerable, but actually the existence of the pandemic itself—people's concern about vaccination, testing, and research—is being taken advantage of at this time.

Jen Rathburn

That brings a lot of issues in because, even though—for example—a nation-state actor is trying to get in to steal actual IP, whether that's an actual COVID vaccine or other related research and testing, but even if they come in and they're not successful, it still causes a breach to your systems. Even if data isn't ultimately exfiltrated underneath the HIPAA rules, it's really important for health care organizations to understand that potentially even that access alone could cause you to have a reportable data breach, so we're just really seeing an uptick in that space.

Brian Resler

Absolutely, and we always say try to take care of these events when skies are blue and the seas are calm, but unfortunately, you have to double down on doing that during times like this that are challenging such as the pandemic.

Jen Rathburn

That's very interesting. Let's get down to the bottom line. What can organizations do today to really “tune up” their cybersecurity program? And I just want to talk about some of the big, quick wins they should focus on.

Brian Resler

First, and I would say this at any time, know your network environment, know your vulnerabilities, and know your assets, and I cannot stress this enough. For example, if you're using Office 365 or some email service provider, turn on multifactor authentication and disable legacy authentication, which would allow people to access your email system using outdated systems. Another thing that I would mention is get an up-to-date network map. This seems to be something that people would think, well, of course we have one on hand, but I can't tell you the number of matters I've worked both as a prosecutor and in my current position where you find out in a business that IT is worried about so many matters in the business that keeping track of which servers and users have been retired or rebuilt, or even where they're located, is just not available and done. So if you could start right there and just take an inventory of what you have and where it is, that will be especially helpful. If you get hit by a breach, if there is a need for an incident response, you're going to need to locate all of that anyway, and that will take precious time and resources away from getting where you really want to be, which is your system set up and your data safe and secure.

Jen Rathburn

I would say, Brian, that's a big issue just on the privacy end. Part of doing any sort of privacy program is really doing a data map of what type of data you have. Clearly as a health care organization, you're going to have protected health information (PHI), but you could also have something called personally identifiable information that would be outside the scope of HIPAA, potentially, that would pick up under state law. You could also have credit card data. Clients really do struggle with doing that data map and I guess I would say, the practical approach is to at least get big items down. Figure out where the majority of your PHI is stored or what vendor has that PHI—similar to credit card data and other sensitive data—because in the event of a breach, you as an outside forensic expert are not going to be able to tell the client what data is on those particular systems. I mean you could, but it's really a hard process post-breach to try to figure out what types of data have been affected.

Brian Resler

To add to those points, and referring to the Department of Justice indictment from a few weeks ago, know where your most valuable information is—your trade secret information, confidential business and research information. Know what servers have that kind of information, know what users may have access to that information as much as you can upfront. It will absolutely speed up recovery.

Jen Rathburn

Most definitely. What are some other tips other than a pure technical side?

Brian Resler

A real easy win is to check your list of current users, particularly those with administrative privileges or administrators. Often we'll find in a system that people have retired, they left the company, servers might not be used anymore, and the administrators involved with those servers aren't even involved in that position anymore. And what happens is those accounts still stay on the system, and the problem is that's now a liability because that account might be able to be used now and not flag any kind of AV protection. It may not be flagged in your firewall, it may look like legitimate traffic, when in fact that old account has now been hijacked by an attacker and is being used for their ends.

So I would also suggest to go through on a regular basis and clear all users who are no longer with the company or your business. Make sure that people's privileges are set appropriately so they only have the authorization and the credentials that they need, and particularly focus on administrative privileges.

Jen Rathburn

That makes sense, and it's working with the HR department and the IT department to make sure that the IT department becomes aware of not only transition of different job roles, but when employees retire or are terminated and leave for a new position.

Brian Resler

Absolutely. This next one goes back to my days as a prosecutor, but it's still true now. I would activate as much logging as possible, whether in your email system, in your firewalls, in your network event logs, et cetera. We'll often find in an incident response that it can be a few days before we come in and we're involved and retained, and believe it or not, sometimes systems are set to literally roll off those logs in a day, sometimes even a week. Ideally, you'd have those logs at least two weeks and maybe even up to 30 days. So I would say, do as much logging as you can possibly afford to do because when we get in and are involved, you might want to know right away the kinds of information that you were talking about that's sensitive—personally identifying information, trade secret information, health information—and whether or not it left your business. And those event logs and those kinds of logs can be one of the first things we can look at very, very quickly and see if information has left the company.

Jen Rathburn

That's really a hot topic issue that I deal with—with breaches all the time—and unfortunately, before forensics gets in, oftentimes systems are restarted and the logs are erased, or they roll off the system, and we end up with a forensic report that basically says, we don't know exactly what happened because we don't have evidence to prove or disprove anything. So what happens in a lot of cases, not just the health care industry, is that you end up having to do a breach report, which is really over-inclusive because of the lack of logging, so I can't emphasize that piece of advice enough.

Brian Resler

And I would add, in our reports, we often have to say, based on the evidence we reviewed, we didn't see signs of, for example, exfiltration. It's very hard to be 100% sure when you don't have all the evidence in front of you that could be there and it just pays dividends down the road. When you're not having a breach, all that logging and all that data may not seem necessary, but believe me, if something happens, you will absolutely want access to as much of it as you possibly can.

Jen Rathburn

Could not agree more. Any other tips?

Brian Resler

As a final point on this part for knowing your network environment, don't just know your environment, but consider what other businesses or entities might have access to your network and do a check on those. Do they have more authorization than they should have? Do they have more credentials than they should have? You may have a vendor and you've created multiple accounts for people who've worked with that vendor over the years—you may need to clear out those old accounts as well. So it's not just your security you have to pay attention to, but also the security of the people you do business with regularly who have some level of access to your network.

Jen Rathburn

That makes sense. One of the things that a lot of our clients have is cyber insurance and it varies in different types of policies and coverage, but what are your thoughts on cyber insurance?

Brian Resler

This is a really interesting topic. Having been a prosecutor who's worked in the areas of investigating and prosecuting cybercrime for many years now, I remember a time not that many years ago when having cyber insurance was a very rare thing. Now, it's coming to a point where, more often than not, we find our clients do have cyber insurance, but periodically some still come through and don't. What I would say is this: breaches are incredibly expensive in terms of time, money, and labor—to not only remediate, but to address legal concerns, to address shareholder concerns, to pay for incident response. It's incredibly expensive and you can easily get not only in the tens, but hundreds of thousands of dollars. Certainly for a lot of businesses already struggling right now with the pandemic and the stresses put on them from that, they have one of these incident responses and not having insurance could be devastating, so absolutely you'd want to do it.

I guess some good news in terms of getting insurance is you'll have to make some network map. You're going to have to do some updating in order to get a policy anyway, so in a way, it really forces some level of internal assessment of your network and your vulnerabilities, which I think pays dividends in both ways.

Jen Rathburn

That makes sense. I mean, one of the biggest things that I see with clients is that they have a breach, they reach out to the cyber insurance, and then they don't know who they can use on their panel, whether that is a forensic firm, a PR firm, a law firm. So I always recommend to all the clients that I work with in advance is not only do your incident response plan, which we'll talk about, but make sure that you get all your preferred vendors on your plan. When you're in a moment of crisis, you want to work with the people that you work with every day that know your business, that know your individuals, et cetera. Do you have any thoughts about that as well?

Brian Resler

Absolutely. When we get called in for an incident response, oftentimes we're learning from the ground. From the very first call we're assessing the network, assessing where there might be holes, vulnerabilities, assessing sources of evidence, figuring out who we need to work with, maybe where the most valuable information is. I can tell you that goes much, much faster if we have a pre-existing relationship, so I would really suggest getting some kind of incident response firm on retainer.

What that will do is allow them to get to know you and your system, and with periodic check-ins, in a best-case scenario, you don't have to use them, but if you do, you will save an unbelievable amount of time and stress because you're reaching out to someone who already knows your network, your system, your vulnerabilities, your assets, instead of having to teach that to them upfront. I can say from working with so many clients in the middle of a breach, it's incredibly stressful, and so the amount of time you can save, the amount of assurance you'll get from knowing that you're working with someone who knows your business, knows your systems, will definitely pay for itself.

Jen Rathburn

All the studies that have come out, they say the best ROI to reduce data breach costs is really to make sure that you have defined your incident response team, and that's your internal team and it's your external team as well. It's also making sure you have an incident response plan and that you practice that through things called “tabletop exercises.” I've been doing this for about 20 years and I'll tell you, that is where I see clients perform the best, perform the quickest, have the least stress, is to just do some of that due diligence on the front end.

Brian Resler

You make a really good point on that because, besides providing those other advisory services and penetration testing, you get to know the team that you'd be working with, not only from the incident response firm, but from the incident response firm back to that internal team. Oftentimes when a breach happens, not only is the business concerned, but for people who might be responsible or take ownership for controlling the network and the end points, there's going to be a high level of stress there, right? Did I do something wrong? Did we miss something? What did I do? And that can create some friction unintentionally between an incident response team and an internal team.

So getting to know each other from the beginning and maybe strengthening those bonds, makes things go much, much smoother when you have to work so closely together. Oftentimes I will go from meeting someone at 9:00 PM at night to a week later feeling like I'm good friends with them for a long time because we've been on the phone and communicating so much over that last week. It really helps to get that relationship upfront as opposed to developing it then.

Jen Rathburn

We're definitely incident responders during high stress, and I will say on that point, what I've seen the most through “tabletop exercises,” it really helps an organization and the individuals that are on the incident response team really understand what their role is. If you practice through mock exercises, it's really helpful for companies to sit down and say, "Okay, in this instance, who needs that upper level approval? Do I want to be involved? Who do I need to go to before we sign off and make any public statement? Who all needs to be in the loop?"

Oftentimes, what's most helpful is it allows the incident response team leader to really take that lead and others that may have higher positions, shall we say, follow under that incident response leader, unless you're going to public notification. It's just so important—when things are flying all over the place, and potentially you could have outside exposure because you've been on Krebs, you've been outed to the public that you have this breach—to really practice and understand each team member's role in order to get out and get an accurate notification out because you're under a lot of pressure with timing to get the notification out.

We know from studies that if you go out too soon without understanding what actually went on, it costs you more money because you're making public disclosures, potentially about things that you don't even have an understanding of internally. For all of those reasons, I definitely cannot recommend more than practicing. I think what would be helpful in the end, for those of you that have not suffered a large-scale breach, is really to understand how the process works and give you a little bit of background.

Normally it's the in-house IT team and attorneys who either find the breach themselves or are notified by a third party vendor. It takes some time to get your feet under you to try to figure out exactly what is going on here. Then, I often get called as outside counsel to try to enhance the attorney-client privilege over the investigation and really act as a data breach coach. They ask, "Well, what do we do next?" and the number one first thing is, "Do you have a forensic firm?" because I always recommend using an outside forensic firm unless you're able to contain that breach yourself and it's minor.

Why? Well, if you don't contain it yourself, which happens all the time and the attacker is still in your system, a few months down the road, it does not look very well, in other words, to the public or regulators that you handled it yourself. You didn't do a good job and the attacker remained in the system. It's never a good story, so I always recommend at least reaching out to a forensic firm to get their thoughts. We hire the forensic firms under attorney-client privilege, we work through those agreements, and then—I'll turn it over to you now, Brian—once I contact you, really, what are the next steps on your side?

Brian Resler

What we want to establish upfront is a very close relationship between ourselves and the legal team, because there's so many decisions that need to be made during an incident response, and some will fall directly on the legal team, some may fall on the incident response team. Often there's a lot of in-between decisions that I think really benefit from both the experience of an incident response team, as well as the legal knowledge and experience from the legal team.

There's a variety of things that we would collaborate on in working on a case. The first and foremost thing that almost everyone asks is, "Did they take anything? And if so, what did they take?" And as we've been mentioning in all the time leading up to this, depending on the information that's taken, you may have reporting requirements, for example, for personally identifying information, health information, or credit information.

You also may have different requirements, for example, to shareholders if you lost company assets, if trade secret information has been taken. You may have regulatory filings that need to be made. Trying to figure out what that information is, what level of proof we have about the information that was taken, and what we can say about that information is often going to weigh very heavily in the decision of whether to report and what to report.

Even beyond that, there's often questions at some point in these, should we notify, for example, law enforcement or the FBI? If we do notify them, what should we say and how do we phrase these things? That can be very daunting for someone who's never been involved in the criminal system, let alone let's say the regulatory system, and certainly having legal counsel working with an incident response team who often has the same level of experience that, for example, some of the FBI technicians may have who'll work on that in those investigations, is going to be really helpful to help you figure those things out.

You're also going to have to do a risk assessment when it comes to prioritizing the order of remediation and rebuilding. Oftentimes we're on parallel tracks. There's one track, which is, “let's try to stand up the company systems as soon as possible and get them operational,” and that's incredibly important for the business. You can't afford to be down for a week or two weeks while you figure this out. You need to be basically building the plane while you're flying it, but at the same time, we have to preserve evidence in a way that's forensically sound. Number one, we want to make sure that the statements we give are completely accurate and completely backed up. But on the other hand, we also want to make sure that we're not missing anything.

The worst thing that could happen is that we're rebuilding the environment, we don't know about some factors out there—there are machines that are missing, things that are connected to the network and somehow that's turned back on later and there are still command and control servers that still can reach out on the system, that there's malware present that we didn't find and eliminate. So, you really want to make sure that when you're rebuilding your systems, you're doing it in a forensically sound way, number one, and also, so it's clean and it's safe.

Oftentimes we'll start out with, and this is a conversation I often have with counsel, is to talk to the client, figure out what is the most important thing for you to stand up right now? Do you have payroll coming up? Is there a sale that the company's involved with, either selling a company or purchasing another company? What are the reports that have to get involved with that? Is there a new product being released? What goes on with that? And you can just run down the list of things that may matter to the company and help them prioritize, what's most important to us now, and try to get that up and running as soon as possible while we work to fix the rest of the system.

Jen Rathburn

I get a lot of questions from lawyers in particular that have concern over notifying the FBI or other law enforcement, and I think that's just a big misconception. The FBI really takes the data and they do it for threat sharing purposes, but the FBI is not going to come out to your organization and get the attacker out of your system. Obviously, if they have information that they already have, they will give you that and share that, whether it's a decryption key or something else, and the FBI does not share information with regulators about your incident. I have a lot of clients that are just hesitant to do that, and really don't understand law enforcement's involvement. I mean, really it's you, Stroz, or another forensic provider that really come in and help them get their systems back up. It's not the responsibility of the FBI or local law enforcement.

Brian Resler

Absolutely. Although notifying law enforcement, as you noted, really pays a lot of dividends. Number one, law enforcement gathers a lot of information and they may be able to give you

information that could be very helpful in standing up your system or responding. But second, when you give information to the FBI, that may also help another business, just like the FBI got information from other businesses to help you. So it's a model that really works for everybody. And as you noted, while they're not there to fix that problem, they are there to try to share information and to assist and not to report whatever happened to other regulatory agencies.

Jen Rathburn

One other thing that is getting new focus as well that I want to mention about ransomware is that you also have to be very careful if you're going to pay ransomware. This is another common question I get from clients all the time: "Should I pay ransomware?" First, the question is, can you back up on your own? Do you even need to contemplate paying ransomware? Second, if you are going to pay ransomware, we really need to do an analysis of who are you paying ransomware to because you may be prohibited by U.S. law from paying certain bad actors in other countries. I think people have lost sight of, well, I'm just going to pay for the ransomware, but you actually could get yourself in a situation and be subject to U.S. legal penalties for paying somebody that is on a list overseas of a nation-state actor.

So that's just a new thing that we've been trying to counsel clients through. Obviously, we don't recommend paying ransomware, but it really depends on the particular situation, whether you can backup data.

Brian Resler

That's absolutely true, and that goes right back to our first point—knowing your network, having an updated map, having teams that know you and know your business is so critical when it comes time to do that. Even the decision whether or not to communicate with a threat actor is something that is going to be very carefully considered by both your incident response team and legal counsel. And I think people sometimes are under the misconception that once you pay, your systems are just unlocked. While it's true in many cases, it's not true that it's a very simple process. Normally, there's a considerable amount of effort and time that still goes through rebuilding systems, even once you have the decryption key. And of course those keys always carry the risk that there may be additional malware inside, so literally, that the cure is still going to infect you with something else, to be very candid about that.

Jen Rathburn

I've seen that happen to a lot of clients. They try to restore on their own and they actually just have bombs in the restoration process that haven't happened again. So one last piece I'd like to cover is the art of really drafting a forensic report. I review them all the time from all different types of forensic providers, and the reason why this report is just so essential,

which I advise clients on all the time, is that really your communications to others—whether that be the effected individuals themselves that had data either accessed or exfiltrated, or if you're a vendor reporting to your customers—is that you really need to base all of your communications on the forensic report and what the forensic report says. I see a lot of clients wanting to go beyond or connecting the dots, et cetera, and it's just really important to convey accurate and truthful information that is derived from a forensic report. If you could talk a little bit about your process and developing those reports, and maybe some of the pitfalls you've seen in the past.

Brian Resler

Absolutely, and whether or not to draft a report and what that report will say often comes up very early in an investigation, even when we don't know what we're going to find. It's always a case of trying to manage expectations by saying, first we have to see what sources of evidence are available. Are there any gaps in those sources of evidence? How much can we learn about the network from logs, host-based analysis—i.e., looking at the machines or servers themselves? And then, really, the critical part is then working with the legal team to make sure we're stating things in an appropriate way for that business.

We always base our reports on evidence, so if we believe that we have evidence for something, we will state that affirmatively, but so often, even in the best investigations, there are gaps. Some gaps are because there's a loss of evidence. Some gaps are just because the evidence isn't that conclusive. So you have to make statements that may suggest, for example, that data may have been stolen, but you can't say much more about it. Or you may state the opposite, that we don't believe in this case that data was stolen based on the following, but a caveat that it's possible that in one of those gaps in evidence, one of the sources wasn't as good as you'd hoped it would be, that there may be something there.

As you noted before, Jen, clients for very good reasons are often very concerned about that. They want to make as strong a statement as possible that nothing was taken, or if things were taken, this is all it was and it was no more than that. That's something we work very, very closely with legal counsel on and usually what will happen is, we will put off any versions of report, or even any hard statements, until the very end of the investigation when we have a good sense of things. We'll then prepare a report from our end, it will be reviewed by myself, and really get a lot of good background myself from being a former attorney and prosecutor in this area.

But the next step isn't really going to the client. It's going to counsel, the legal team, because legal may know of other concerns that our incident response team doesn't necessarily know about. And maybe it's not even a role to play in that matter, but elaborating a little bit on a piece of evidence that we found and what its meaning may be, or backing away from something on another point, may be the best strategy going forward.

Jen Rathburn

But that's the part right there, I think, where the intersection between forensics and legal is so important for people to understand, because it really depends on each organization. For example, and one of the things I would say a lot of the insurance panel experts is, they're generally good across the board, but many of them don't have deep insight into things, for example, of HIPAA. HIPAA's rules on when you need to report for a data breach are very different than state data breach notification laws. Many health care institutions also may receive data that's governed under Department of Defense rules, currently 800-171. Those standards are very broad on reporting.

Also, there could be, if you're an international organization, GDPR concerns which have 72-hour notice. So, when we work together, that is just so critical to make sure—you need the legal understanding of when an event or an incident actually triggers into something that you have to notify and what laws you need to notify under.

I think that, when I work with a lot of clients, they don't really understand that certain events may not be reportable depending on the facts. I really encourage organizations to not scream breach through email correspondence to others because oftentimes something does not need to be reported. And the alternative is, depending on your organization, you may have to report things that wouldn't seem to be a breach—there's over-reporting requirements. For example, under the DOD, if you do any type of research in that area, if something hits your information systems, you have to do notification. So I just think that is a very critical piece.

I just wanted to say thank you so much for talking with us today and your profound expertise in this area. I wanted to leave with just one last mystery question for you, Brian. What is your favorite part of your job and why are you so good at it?

Brian Resler

What I like about my current position is actually the exact same thing I liked about my last position as a prosecutor—that ultimately, although we're talking about cybercrime and affecting businesses, and we're all worried about these kinds of risk management and the kind of experienced judgment calls we need to make, ultimately, it's a very human endeavor. I like most working with people on the other end of the line and knowing that we're helping them and being involved with them, because each of them is a person—they have jobs, they have roles within their company, they have families to care for—and interacting at that level makes all of this high level talk, frankly, worthwhile.

Because there are days when I hear the number of acronyms being thrown out about a particular network and system and we have these high-level discussions about reporting, and it's easy to get a little lost in that, but realize when you're connecting with people and

really working with them to try to make their systems better, to make the best of a bad situation is really what makes this worthwhile for me.

Jen Rathburn

And you're fantastic at that. So thank you again so much for your time today, and now I'm going to turn it back over to Judy.

Brian Resler

Thanks so much, Jen – my pleasure.