# Ransomware: what boards need to know about the Colonial Pipeline attack

The following is a transcript of the Freshfields podcast *Ransomware: what boards need to know about the Colonial Pipeline attack*.


**Boris Feldman**

Partner, Silicon Valley

**Giles Pratt**

Partner, London

**Kimberly Zelnick**

Partner, New York

**Nabeel Yousef**

Partner, Washington, DC

**Lauren Honeyben**

Partner, London

**Brock Dahl**

Counsel, Washington DC/
Silicon Valley

**Shannon McGovern**

Counsel, Washington, DC


---

**Boris Feldman**

Welcome everyone to this latest podcast from Freshfields Bruckhaus Deringer. Today's topic is ransomware attacks: what boards of directors and senior executives need to know about Colonial

Pipeline and similar attacks that may be coming. Usually we focus these podcasts on our clients and friends in legal departments. This one is aimed a little bit more at the board of directors and the C-suite, although obviously our legal clients are more than welcome to join in.

I'm Boris Feldman, I'm a lawyer in the Silicon Valley office of Freshfields, and rather than introduce a bunch of people to you now that you'll forget by the time they talk, I'm going to introduce you to our colleagues as we hear from each of them. So, we're going to begin with our newest colleague, Brock Dahl, who's resident in both the Silicon Valley and the Washington, DC offices. Brock joined us recently from the National Security Agency where he was deputy general counsel for operations. So if you hear any strange noises during the recording it's probably his former bosses checking up on him.

Brock, welcome to the firm. People have probably read a lot about Colonial Pipeline, or they've listened to it as they've waited in line for gasoline. Could you give our audience the salient facts, and maybe things they might have missed on the Drudge Report.

---

**Brock Dahl**

Thank you Boris, it's exciting to be here. The Colonial Pipeline Company manages about 5,500 miles of pipeline that's distributing gas and jet fuel across the Southeast and East Coast of the United States. On May 7, Colonial announced that it was shutting down its operation, meaning that that fuel would no longer be running through that 5,500 miles of pipeline. Now, while there wasn't a lot of information available at first, on May 10 the FBI announced that the company had been the victim of something called the Darkside ransomware. Now Darkside is a ransomware-as-a-service platform. It's a bit of a unique animal in the breach space – it's a construct where criminal operators create a ransomware and then look for partners in order to take advantage of companies and distribute that ransomware. The partners that they seek to work with will, in some fashion, already have access or will develop access to the company, and then once they have that access will deploy the ransomware in order to seek a ransom. And what we know about the Darkside ransomware is that it's a double extortion model, typically. That's one ransom that's requested for a decryption key in order to free up your systems, and then a second that's requested in order to return or destroy any information or data that was potentially exfiltrated from the systems. All we really know about right now with respect to Colonial was that there was the first stage of that approach in order to seek decryption.

---

**Boris Feldman**

Let's go now to London to our colleague Giles Pratt, who's head of Freshfields' intellectual property practice and has been involved with many clients on data and cyber issues.

So Giles welcome. Imagine that you're a senior executive of a company and your chief information security officer texts you that someone, or some group, has penetrated your information systems, launched a ransomware attack and is demanding a payment. What should you do as a senior executive from that first notification?

---

**Giles Pratt**

Thanks Boris, well this is really the ‘press the red button moment’, and a time to get your core team around you to engage your cyber incident response plan. Obviously the priorities are going to be to contain the incident as best you can; you do hear stories about people running around to pull the cable out of the computer, it’s not exactly like that but people will be trying to limit the effect of the ransomware as best they can. Then it’s really about making sure that you’ve got key lines of communication among all of the stakeholders that you need around you. It’s IT, it’s your cyber security team, it’s legal, investor relations, PR and at some point, it’s going to be the right time to tell the board. Once you’ve got that team up and running, you’re going to want to understand what systems and data are at stake, you want to review your systems and your position on backups, and you’ll want to think about what you’re going to do over the next 24 to 48 hours. That might be engaging with forensic vendors, external counsel, thinking about what other communications you’re going to have to make externally, including obligations to notify regulators, how you’re going to engage with law enforcement, and also you want to think about your insurance position. So there’s quite a lot to do.

---

**Boris Feldman**

This is an uninformed question. How can you do that on the firm’s IT systems if you don’t know whether the intruder’s watching?

---

**Giles Pratt**

It’s a great question, I’ve heard some people effectively want to take their communications dark using a second line of comms in that type of incident. But really we tend to see that people want to use their normal lines of communication because that is most efficient, but also they will pick up the phone, sometimes the old ways are the best.

---

**Boris Feldman**

So I want to shift now Giles from the executive, the C-suite level to the board level. And now Kimberly Zelnick in our New York office who’s the senior person in investigations and has done many cyber breaches and intrusions when they’ve surfaced for clients.

Kim, you’re now advising the board, you’re a member of the board - what are the first things you should ask management and what should your role as the director be?

---

**Kimberly Zelnick**

I think one of the important things is not to treat it any differently than you would if it was a different kind of situation. You should feel free to ask questions even if you don’t think cyber is in your wheelhouse, it seems technical. You want to know what’s happening in order to address the situation - who’s in charge, what’s happened, what are we doing to address this? Don’t be scared

to ask technical questions to make sure that you're really getting under the hood. Because ultimately as a director you have a duty of oversight, you have duty to understand and to be informed, and so that when you're making, if you're giving authority, if you're advising management to go ahead with their action plans that you've done that from an informed basis.

---

**Boris Feldman**

Sometimes companies are a little reluctant to put out the bad news about a breach because they're worried about spooking their users and getting hit in the market.

What role do you think the board can play in probing a non-disclosure decision by management?

---

**Kimberly Zelnick**

As folks will know, there are circumstances in which there is a notification obligation, for example you can have a GDPR notification obligation where you have to, notify European regulators if you have European consumers who's personal data has been affected. But there are other circumstances where notification may not be required, and so understanding that folks had done the right analysis to understand whether or not there's a mandatory obligation to notify or not. But on top of that, if there's a decision not to go to law enforcement for example, which may be totally appropriate, understanding what's motivating that. And fundamentally what you really want to know as the director is that management is doing the right things.

---

**Boris Feldman**

One more question for you on the board-level reaction.

Can you envision any scenarios in which the board would need their own technical advisor on the breach of remediation issues, and if so, what should a director look for in deciding whether or not she should ask for the board's own advice?

---

**Kimberly Zelnick**

If it's a bet-the-company kind of breach, where you just know invariably that there's going to be losses on the other side because the breach is so significant, it's headline grabbing, a lot of people's data has been affected, then you very well might want to have your own advisors. But oftentimes that's not necessary Boris and in fact it's perfectly acceptable to rely on the advisors that the company has retained.

---

**Boris Feldman**

We're now going to turn to the 64,000 dollar question, regrettably it's probably the 64 million dollar question, and for that we're going to go to our money man, Nabeel Yousef, a partner in our Washington DC office who heads our US sanctions and export controls practice. An area that might not immediately come to your mind when you're thinking about a ransomware attack.

So Nabeel what should management and the board think about from a regulatory and statutory standpoint in deciding whether or not to pay the money?

---

**Nabeel Yousef**

Thank you Boris, yes there are a lot of things that companies should think about when the question comes up on whether or not to pay a ransom and that includes that the lawfulness of the ransom payment, practical challenges to actually making the payment, reputational harm, the potential contractual impacts. There are a number of legal regimes in the US, in the EU and the UK abroad that a company should take into account when it's considering paying a ransom. First and foremost of those are going to be the sanctions rules. Actors in this space are often going to be not exactly the good guys, and oftentimes they can be included on sanctions lists. The sanctions regulators are admittedly a little bit behind on adding them to sanctions lists, but if the recipient of a ransom is on a sanctions list then the US sanctions rules, EU, UK, Japan, Canada, could actually be a factor in deciding whether or not to pay a ransom. And the expectations from regulators on the due diligence the companies are going to do into the recipients of a ransom payment is accelerating dramatically And that's just going to put companies on more and more notice, that if they're paying a ransom they have to be aware of who they're paying it to as much as possible - sometimes you just can't – and figure that out. If the recipient of a ransom payment is a sanctioned person on a sanctions list, or located in a sanctioned country, there are things though that companies can do. They can meet with the regulators, they can talk to, for example in the US, OFAC in the US Treasury Department. They might even need to go and get a specific licence from OFAC in order to pay a ransom. This is still very much a space that's developing and the regulatory guidance is not as complete I think as even the regulators themselves would like it to be. On a related note, as Brock had mentioned earlier, in a ransomware attack it's also entirely possible that data could have been exfiltrated to the extent that foreign persons could have had access to export controlled data on a company's systems. There's a whole separate set of considerations that would need to be taken into account with respect to potential mandatory or voluntary disclosures. There's certain access by certain foreign nationals to, for example defence trade-controlled information that would require a company to do a mandatory disclosure. So there's a lot of things to think about when considering whether to pay a ransom as well as to consider when it comes to potential regulatory disclosure obligations.

---

**Boris Feldman**

So I don't want to get into the moral issues about 'is it right or wrong to pay the ransomware. But I wonder Brock if you have a sense, in general when companies are hit with a ransomware attack, do they usually pay, or do they usually not pay?

---

**Brock Dahl**

There's a lot of great reporting out there, Sophos, the cyber security company just did a report about the amount of organisations that pay, and in fact in the Colonial case it's fairly applicable since the highest percentage of those who pay are in the energy [and] oil and gas sector. Now an additional question to ask, is the actual effectiveness of the payment. So when dealing with these criminal organisations, the executives and the board needs to ask themselves, "How high a confidence do we have that when we make the payment we're actually going to be delivered decryption keys that work?" And in addition to the reporting about payments, there's increasingly data out there about the yield on these payments. What's the percentage of success when we make these payments? Decision makers should really review that data because the evidence is mixed that you actually get what you're paying for.

---

**Boris Feldman**

I'm going to put Giles on the spot because he's the senior person on the podcast. If you were on a board, would you adopt a general rule or a very heavy presumption that you would not permit the company to make a ransomware payment, or would it be more of an individual incident-driven analysis?

---

**Giles Pratt**

It's a great question, and actually I think most organisations take the view that they don't want to engage with ransom demands in that way. The challenge though is where you are looking particularly at organisations that have a critical role to play in infrastructure, and where they may not be prepared in terms of the backup resources that they can bring to bear, there they find themselves in a very difficult squeeze. We have seen examples recently though where even in a healthcare situation, governments have effectively resisted ransomware demands. And so actually you will see I think quite a trend towards people wanting to say "no", because they don't know where the story ends.

---

**Boris Feldman**

On the topic of whether to pay, let's turn to the related question of who pays. And we're going back to London to our partner Lauren Honeyben who's one of Freshfields' resident experts on insurance.

So Lauren give us the environment on ransomware coverage now, which I think may be evolving week to week, and any tips that you have for senior management and the board, on the right way to engage with your insurance companies.

---

**Lauren Honeyben**

Thanks Boris. so let's start with the situation where you do have cyber insurance. It might seem obvious, but the first thing to do is to check whether a ransom payment would be covered by the insurer. So broadly, insurers have taken the rational economics approach – so it's better for them to pay out a smaller amount now than a larger amount in the future if the ransom payment isn't made. For the most part, insurers do cover ransom payments, however there's a growing political and social pressure on insurers in some countries to stop these payments, and just recently we've started to see some insurers pull this cover for public policy reasons.

But if you do have cover, the key point is that the insurer does not make the decision about whether to pay extortionists. The policyholder makes the final call, and if that policyholder does decline to pay, the insurers should support it.

In addition to ransom payments, most cyber insurance policies will cover your costs of investigating the incident, recovering data, the restoration of computer systems and other loss of income incurred by the business. And sometimes they can also cover third-party coverages, so the cost of legally defending yourself against claims of a GDPR breach and third-party financial and reputational costs.

Another point I think is worth highlighting is that insurers often provide staff to negotiate with hackers and other IT and PR services as well. But not to worry if you don't have specific cyber insurance – it's also worth checking whether you've got cover in your property liability or general liability or D&O insurance as well. Although these can be often silent on whether they cover the consequences of cyber attacks. In any event, there will be notification requirements, so you'll need to contact your insurance providers to inform them of the attack.

And I think it's important to note that cyber insurance can be a valuable component part in a larger risk-management strategy. So for example the insurance underwriting process itself is fairly rigorous and raises awareness of cyber threats and identifies how you should be responding so it can be helpful in the round as well. If you're thinking about taking out cyber cover for the first time or renewing, the best strategy really is to prepare and engage early for that renewal process, so if I'm advising a board what do in thinking ahead in terms of cyber risks, that early engagement is really key. We're seeing a really sharp increase in premiums and retentions for cyber policies, so in 2020 the average premium increased by 28%, so it's pretty high and part of the cost-benefit analysis that you need to think about when you're taking out cyber cover. And the more incidents there are, the more rigorous you can expect the underwriting process to be.

---

**Boris Feldman**

Okay, thank you Lauren.

We're now going to turn to the regulatory and law enforcement side. And Kim, in addition to investigations you do a lot of white-collar and enforcement work. We've heard a little about this from Nabeel and Brock, but from your perspective, from the time your client learns of the intrusion and the demand, how should they interact with the regulatory and law enforcement authorities in what we'll call in air quotes, "their home country", their headquarters country?

---

**Kimberly Zelnick**

I think first of all it's important to consider of course if you have a mandatory notification obligation. So under European rules you might have a very short window under which you have to notify folks that there's been an incident. But putting that aside, there's a question of, "Do we call the FBI in the United States? Do we make a report, whom else do we tell?" A lot of times, there are separate determinations that you have to make, and what is the purpose of engaging with law enforcement in a particular jurisdiction? Is the FBI going to be helpful? Are they going to be focused on just finding the bad actor, and will that interfere with what the immediate objectives are in terms of securing the environment, notifying consumers. And I think that the mistake that people most make is thinking that they have to make all of these decisions immediately, as opposed to thinking through the different regulatory environments and the different jurisdictions, when folks would expect to hear from you, and also why are we calling now? What are we going to be saying? What information do we have to provide? And in fact, while some decisions need to be made very, very quickly, other decisions can be made a little further down the road with the benefit of more time and reflection and understanding what it is we hope to achieve with a different regulator.

---

**Boris Feldman**

Is it your experience, having dealt with companies in these situations, that they're appropriately focused on regulatory authorities outside their home country, or do they tend to forget about the other geographies perhaps until later than they should?

---

**Kimberly Zelnick**

I think that's exactly what happens sometimes Boris is that people get very focused on just the notification obligation and they don't think more broadly about whether they may have other regulatory, soft or hard, obligations. And so thinking about it in the round, and thinking about all the different jurisdictions and taking in assessments, and again not feeling necessarily that you have decide everything in the first 72 hours is really important. And having a strategy! Different regulators are going to have different desires for how much information they want, how much they even want to know. And so to thinking about every regulator and where they fit, and what your relationship is, how many customers do you have in that region, are you a regulated entity, that is going to factor in to how you're going to approach these kinds of circumstances.

---

**Boris Feldman**

Coming into this recording session, I would have assumed that when a company is hit by a ransomware attack, the government views the company as the victim. Giles has that been your experience?

---

**Giles Pratt**

I think it depends on which authority you're looking at. So there are organisations out there, that are really there to help, so for example in the UK, you've got the National Cyber Security Centre, they see themselves as intelligence gathering, sharing, giving advice, trying to coordinate with other similar authorities around the world. There are other authorities that are there really to assess how well you've done, so Kim has alluded to the data protection authorities in Europe, whether it's personal data at stake in a ransomware attack. And in that situation when you notify the data protection authorities, they're probably going to look at the incident as really a possible symptom of something underlying which is not right within the organisation. So the questions that they'll be asking, "is this really just a bad thing that happened to a good person, or was there a reason why the attacker got in?" And we see time and time again authorities using incidents of whatever nature - ransomware is obviously a very timely example - as a way of probing an organisation's general security protocols, understanding what measures they have taken to ensure that their cyber security posture is up to standard and thinking about how organisationally they've put themselves in a good place so that they know how to look after people's data.

---

**Boris Feldman**

Before we get to the issue 'public disclosure', I want to stick with 'company as victim or something else'.

Brock first, how often do you think these attacks involve someone on the inside? Is that just something in spy novels, or is it a real problem for the companies that have significant cyber breaches?

---

**Brock Dahl**

Based on the public reporting it continues to be the case that the vast majority of data breach scenarios involve an insider. Now the rise of ransomware and the "crime-for-hire" phenomenon generally can be disconnected from that. You do have the ransomware gangs relying on inside information, but that may be information that was acquired through malfeasance on outside actor's parts, not by anyone on the inside. Nonetheless when you look at the overall pie and ransomware by outside gangs is just part of that pie, the insider threat continues to be a very significant problem with which entities must grapple.

---

**Boris Feldman**

In many areas of investigation, companies like to have the outside experts retained by outside counsel so that they can assert a work product privilege. Do you think that matters so much in a cyber-attack or not to worry about it? Kimberly.

---

**Kimberly Zelnick**

It's a complicated question, and part of it is Boris is that people expect that when outside counsel retains an outside firm to do their cyber investigation that that's going to be privileged. That's not actually necessarily the case, the rules are complicated, they vary by jurisdiction and even if something would be protected in the United States it doesn't mean it would be protected in the UK and vice versa. Generally whenever you're conducting an investigation you need to be really thoughtful about what you're putting into writing because it very well may see the light of day, and so don't assume that you're going to get that privilege protection.

---

**Giles Pratt**

If I can really just second your thoughts that, one of the big mistakes that lots of organisations make in the immediate aftermath of an incident is not thinking holistically across the world about where all of their documents that they create are going to go. And the really easy play from all of the authorities - particularly those in Europe and the UK - is "please provide to me a copy of all of the reports, interim or otherwise, that have been prepared in connection with this incident". And they're thinking about their own privilege rules, they're not looking for example to the US to see if it's a protected work product. And they will expect disclosure if it is not privileged in the local sense.

---

**Boris Feldman**

I'd now like to broaden the discussion beyond just ransomware attacks to cyber breaches more generally. And Giles and Kimberly, how involved should the board be in that process, in investigating, in remediating. Is that best done by the full board or is it a select group or committee? How should they prepare in advance, and then how should they triage the situation when there is a breach?

Giles do you want to try first?

---

**Giles Pratt**

Typically I would see that as being one sponsor at board level for the incident response. What you absolutely don't want to do is to slow everyone down by having too many cooks. But absolutely there is value in showing in an investigation that there is a senior stakeholder who takes responsibility for, and is checking in at the relevant milestones throughout that investigation.

---

**Kimberly Zelnick**

I absolutely agree with Giles, you don't want to create a situation where you're slowing everybody down. That said, the whole board should be interested, particularly if it's a very significant breach and should ensure that there are updates, and really keeping track of having a sense of the overall situation.

---

**Giles Pratt**

And there's a point isn't there, that at the end of the incident really taking stock of what the organisation has learned, how you're going to implement that in terms of how they roll forward their governance and making sure that they are as well prepared as they possibly can be should something happen again.

---

**Kimberly Zelnick**

Yes absolutely, too often there's a tendency I think to say, "great we're done, it's behind us", but oftentimes you can have a smaller incident and you could find yourself unfortunately in that situation again. Sometimes not even that much later. And so whether or not you took the appropriate steps to remediate, coming out of a smaller incident, could be very significant, and if you don't take the right steps could really become a problem down the road.

---

**Boris Feldman**

Potentially there's a broader lesson to be drawn from the points that you two just made. If you've watched movies about space ships from the United States, whenever something goes wrong they ask Houston for the procedure. Some boards actually have a similar process, and it's not limited to cyber, it may apply for an investigation of misconduct by an executive, or to a financial enquiry into revenue recognition issues. And rather than wait until the problem hits the fan, they actually have set in place procedures in advance for how they're going to do that. Independent firms that they can go to and pre-position to handle the investigation. It seems to me given how quickly your cyber problems arise, more so even than an accounting issue typically, or some kind of misbehaviour issue, it might be appropriate for a board to say, "let's have a NASA-like procedure in place for an intrusion, and let's do a dry run and know whom we're going to call and what the chain of command is".

I want to turn to liability, first we're going to do potential shareholder liability, and then we're going to talk about users and consumers. And for shareholders I'm very proud to welcome our colleague Shannon McGovern from the securities litigation practice in Freshfields' New York office.

So Shannon welcome, with respect to cyber breach and ransomware, how big a risk is that to directors of the company, and what situations put them at greatest risk?

---

**Shannon McGovern**

Thanks Boris. So we've already seen in recent years that one of the areas that shareholders have been focusing on and bringing claims against directors, are for perceived failures to properly oversee company risks. And in the cyber security context that would mean allegations that the board did not properly implement its duties to make sure that there was a protocol in place sufficient within the company to identify and mitigate risks, or if there was such a protocol that the board did not act in accordance with its fiduciary duties to the company and its shareholders by properly overseeing that protocol.

There are other kinds of claims that are possible as well against directors, though perhaps more likely to be brought against management as opposed to the board, and those would include securities, class actions or enforcement actions regarding disclosure. So let's say a significant data breach occurs of some kind, there's bad press, there's a stock drop that results. A shareholder maybe bring a suit alleging that the manager of the company and its board misled investors in prior public disclosures about the risks of such an event happening, or perhaps did not provide full and accurate information at the time of some disclosure of a breach or incident that actually occurred.

---

**Boris Feldman**

There are many fake ransomware overtures where companies for some period may be getting notes from somebody saying, "we're going to break in", or "we're breaking in", or "we've broken in". How big a problem do you think it is from the liabilities stand point, if it turns out that the company had been warned about a potential ransomware attack in the past?

---

**Shannon McGovern**

I think that a shareholder looking to bring a suit against the directors will be laser-focused on trying to identify red flags, that the board should have been aware of that at an earlier point in time, so something like you describe would be the exact kind of thing that they would want to put in a shareholder complaint to allege that the board was not living up to its duties of oversight in monitoring the company for those risks. So I think it's important that, as Kim said earlier, the board makes sure that it informs itself of the issues in this cyber security space and has a dialogue with management who'll be primarily responsible for making sure that the appropriate protocols are followed to help address any future claims that the board was not doing everything it was supposed to as the entity charged with overseeing the company and its significant enterprise-level risks.

---

**Boris Feldman**

Thank you Shannon. Let's shift from potential shareholder liability to collective claims by users or consumers.

How big a risk is that to a company Kimberly, and how do you see that risk playing out in the US versus the UK and the EU?

---

**Kimberly Zelnick**

Certainly the US remains the hot spot of this kind of litigation Boris, there's just no question about that. But one of interesting dimensions of data and cyber incidents has been that oftentimes a lot of the regulatory action, and a lot of the investigations will precede that, and they'll take place in Europe and in the UK. Oftentimes what you'll see is, you'll develop a record with data authorities outside the United States, and then that will become the basis for litigation that you will really be

led out of the Unites States. But I don't want to suggest that it's only the United States where we're seeing these kinds of collective actions, for example there's been recent significant litigation in the UK that's been launched, but there's also places like Canada, Australia, the Netherlands where there really are significant consumer class action risk. Then it's also a "watch this space" situation because as folks may know, in the EU there is legislation coming onboard in 2022 that is going to make it a lot easier to bring these kinds of collective class actions on the back of cyber breaches.

---

**Boris Feldman**

I want to close by getting all of your free advice to your niece. Imagine that your niece has just been appointed to the board of a significant public company, and she says to you, "OK, I've been reading about these gas lines in the Unites States and these ransomware attacks. How should I handle myself as a director? what's the right approach on this, I did not work at the National Security Agency," your niece says, "so tell me what I need to do."

Let's start with Shannon. What would you advise this new director about things to do in advance that will give you a record that you're very comfortable defending in the Delaware Court of Chancery?

---

**Shannon McGovern**

Well I think the answer depends in part on the role that the due board member will be assuming. So every member of the board, regardless of the committee appointments, he or she may have as a general duty to oversee significant risks facing the company including the cyber security risks we've been talking about. But that obligation is heightened for folks who are on a committee charged with elements touching on this, so a risk management committee, an audit committee, maybe even a dedicated technology committee of some kind. But regardless, it's making sure I think that the board understands what the company is already doing, gets frequent reports from the appropriate people – whether that's a dedicated security information officer or someone else – and does their best to become reasonably literate in the issues. I don't think there's an expectation that everyone's going to have the same level of familiarity with the technical issues as the managers charged with overseeing these things day to day. I think it's common that new board members have a bit of a long period where they're getting to know the company - perhaps its industry if it's new to them – and in that context cyber security should be one of the things that they put on their to-do list to make sure they understand the environment, particularly facing the company that they will be hoping to oversee.

---

**Boris Feldman**

Good advice Shannon.

Nabeel you've spent a lot of time with boards in very messy situations. How would you advise your niece or nephew about a BS detector? What would you say to her about when her normal reliance on, and deference to, management perhaps should be tempered because the story might not be right. What would you tell them?

---

**Nabeel Yousef**

Well Boris I'd tell her to take a look at the regular regulatory compliance risks assessments that the board probably reviews for the company from time to time, and think really hard about whether management is actually taking all of that into account. If the company has defence contracts or has technology that is export controlled or is particularly high-risk or sensitive, obviously they need to be thinking about that. And also thinking about whether you should challenge management a bit on the identity of the party that is demanding ransom. Simply saying that the party is not identifiable is going to be fine in certain circumstances, but really putting pressure on that and testing one's BS detector on whether or not the ransom recipient is truly unidentifiable, or if they are identifiable, whether they are actually a party that the company from a legal or reputational perspective would want to pay a ransom to.

---

**Boris Feldman**

That again ties into the notion that it's probably good for our clients to think through these issues before they get that text at 4am saying "they're in".

Kim let's say it's your cousin, we've promoted the relative now, it's your cousin going on the board and she asks you, "Should I periodically bring in folks to do almost an audit of our cyber procedures?" Is there a role for that? Is that more of a management role versus a board role? What can she point to, to establish that she was paying attention and not ignoring red flags?

---

**Kimberly Zelnick**

It's almost like Nabeel was saying, it's almost like anything else, you shouldn't treat this as something that you don't want to touch, or its too technical or "I don't understand it". You want to really be able to get in the hood and ask questions. And I think the best way to get comfortable is to probe and to ask the same kinds of questions you would in a different situation. If we are auditing other kind of things, why are we not auditing this? Similarly, if you read about an incident in the newspaper, Colonial Pipeline, what are we doing to ensure that we don't have that kind of catastrophe here? And again asking, I think very importantly Boris, before there's an incident not when you're getting that call at 4am so you actually understand what it is that the company is doing. So you going to be more sophisticated when you get that call at 4am - you're going to know who the names are hopefully of the people who are in charge of handling this at the company, you're going to have a sense of what it is we're doing, what we think our exposure is, what we

think our risk is and I think that that's one of the reasons why even if the answer is, "we're not doing an audit" well why aren't we doing an audit? You are really pressing people to understand are we doing the right things in order to safeguard against these kinds of problems.

---

**Boris Feldman**

As most of you probably know in the Old Testament there are two occasions in which the text discusses the blessing and the curse. So of course we are going to end with that, Brock being the blessing and I think Mr Pratt will address the curse. Let's do the blessing part first. Brock, as an observer of many breaches from the government's side, do you have any examples of a company that's really handled it right?

---

**Brock Dahl**

I think you can look at – and this may be no surprise – FireEye's handling of the beginning of the Solar Winds event. And in particular, their communications at the beginning of the event, the communications that addressed things like, "what do we know, what do we not know, and what's the timeline for answering the unknowns?" A lot of times companies face problems in the market simply because of uncertainty and we saw that playing out here with Colonial Pipeline. The second thing you saw demonstrated with FireEye's particular handling was the result of preparation in advance. So to the point that you made earlier - what do you have in place that will permit you to run through scenarios quickly, and have you planned for those different scenarios?

---

**Boris Feldman**

Giles you know I don't think you're a curse at all, but you've been through many of the largest incidents globally. What is the one thing that you've seen a company do whether it was one that we were involved in or not that you drew a lesson from it and you said well they never should have done that. What's the one piece of negative advice you'd give in terms of, "don't make this mistake"?

---

**Giles Pratt**

Well Boris if you'll forgive me mixing up my curses and my commandments, really I think the issue is whether you are coveting your neighbour. The problem that we see is that lots of organisations benchmark their cyber security posture against others in their sector and actually the world will judge them against what they should have done even through their neighbours weren't doing enough. So the question is how to look to the right standard and there are lots of great reference points for that and frankly Brock is the authority for many of them.

---

**Boris Feldman**

Thank you it’s a pleasure to have you all join us today. If you have any follow up questions you can reach out to our cyber experts around the world. Thank you and have a good day.