"Leaders need to be particularly prepared for the fact that you're really not going to know very much about what happened, who did it, what got stolen, or what broke down – at a point where you may have to start communicating about it. And it may be to business partners, it may not be publicly, but you still need to be able to demonstrate that you're on top of it even when you don't know very much. And that's a very uncomfortable place for corporate leaders to find themselves."

MARCH 16, 2020

Bouncing Back: Advice for Minimizing Reputational Damage from a Breach

Presenter: Siobhan Gorman

Summary

Strong cybersecurity leadership is truly tested when the organization is breached and when it comes to recovering from the damage, the response and public handling of the situation is just as important as the attack itself. Brian meets with Siobhan Gorman, Partner at communications firm Brunswick Group and former Wall Street Journal correspondent, who provides listeners with key takeaways and lessons learned from incidents past.

Transcript

Brian Contos:

Welcome to the Cybersecurity Effectiveness podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness. I'm your host, Brian Contos and we've got a really special guest today. Joining me is Siobhan Gorman. Welcome to the podcast, Siobhan.

Siobhan Gorman:

Great to be with you.

Brian Contos:

So, Siobhan, I have a lot of questions I want to ask you today, particularly around reputation and how to deal with that when there's some type of cyber incident. But before I get into those questions, I'd love it if you could give our listeners a little bit of background about you and how you got into cyber and what exactly it is you do today.

Siobhan Gorman:

Sure. Well, my day job now is, I'm a partner in the DC office of the Brunswick Group, which is a strategic communications firm. And I co-lead our cybersecurity and privacy practice here where we help companies both prepare for and respond to cyber incidents as well as help them take a leadership positioning or address public affairs issues when it has to do with a cybersecurity or technology policy. My route here was somewhat circuitous and kind of depends on how much time you have, so I'll try to keep it a little bit brief. But my background is as a reporter and so that was how I came into cyber security. I was probably about 10 plus years ago, almost 15 actually. I was a reporter at the Baltimore Sun in the Washington DC Bureau covering. And the National Security Agency is in the Baltimore Sun's readership area.

Siobhan Gorman:

So, I spent a fair amount of my time covering the NSA along with other intelligence issues. And at the time, this was about 2006 or so, NSA was perhaps the only, or at least the main agency in the US government, that was really focused on cyber security issues. And in fact, they were working on something that became known as the National Comprehensive Cybersecurity Initiatives. So, I came into cyber security issues somewhat backwards, depending on your perspective, just kind of through that narrow lens of what the NSA was up to. But it turned out that they were really up to quite a lot and there was a fair amount to write about. And when I switched from the Baltimore Sun, to The Wall Street Journal, I told my editor, "Yes, I'm going to cover intelligence for you, but I think that an important part of that should really be cybersecurity." And they said, "Well, really for a business audience, does a business audience care about this?"

Siobhan Gorman:

And I said, "Yes, I think a business audience really should care about that." And they said, "Well, prove it." And so I kind of had this on my first year at the journal while I was covering other areas and issues and things like that, showing them that cyber security was a real issue, it was something that a business audience should be interested in and educated about. And it did take a while, but it was ultimately probably too successful. And I spent much of 2009 covering cyber security along with the other issues I was covering. And so, eventually I persuaded the powers that be there that it should really be its own beat.

Siobhan Gorman:

And so, we created a cybersecurity beat and then I worked with that person when it intersected with national security. So, I've done... been sort of observing intently for quite some time. And then, four years ago or so I switched from journalism over to communications. And as I tell some of my clients, I sort of went from being from their perspective at least, part of the problem to part of the solution. And so now the companies are quite up on cyber security issues. Those who want to prepare for, or sort of respond responsibly are the companies that we're working with day in and day out when it comes to preparing for potential cybersecurity incidents.

Brian Contos:

So, that's a really fascinating background. I'm always intrigued by how people get into this space and you coming into it from a journalist perspective I think definitely gives you a different lens than most, which I think is quite unique. And you mentioned earlier on, some of the things that you do with reputation, we've talked a lot about a lot of different facets of cybersecurity on the show, but one of them we really haven't covered is, what are the risks to a company's reputation in a cyber crisis? So, maybe you could give us some background on that.

Siobhan Gorman:

Sure. Well, there are a number of risks and I think that one of the things that we see companies do, sometimes is... I guess the first one I'd highlight is companies that make missteps in their initial response, particularly ones that make it appear that they're downplaying the issue or not taking data security seriously, or insufficiently focusing on customers, say if they're sort of the ones who are most affected. The second I think is providing details that they then ultimately have to correct a few days later. So, putting out so much information that you know in the name of transparency is good. But if you put out information that then has to be corrected later, then all you do is risk looking like you don't have control over this.

Siobhan Gorman:

I think the third is focusing on the wrong stakeholders. So sometimes companies can be so focused on how this is going to affect the bottom line that they focus on say investors instead of customers, or employees or whoever sort of the real focal point is of the incident. And then I think a couple of other risks are ones that may be companies have a little less control over but should be aware of. And that would be employees who weigh in publicly on social media, or somehow kind of contribute to the overall public discussion in ways where maybe they think they're being helpful, but ultimately, it's not helpful. And another would be when customers start complaining publicly, those are some of the challenges that they run into.

Brian Contos:

Yeah, that makes a lot of sense. You know with... everybody has a bullhorn today, right?

Siobhan Gorman:

Exactly.

Brian Contos:

So, whether it's ... and as we all know, when there's something negative to say, they tend to speak a little bit louder. Tell me what some of the more mature organizations are doing as it's related to this. How are they helping to reduce that risk?

Siobhan Gorman:

I think the most important thing you can do is prepare, prepare, prepare. And that preparation can take a couple of different forms. The first I think is just having a plan but having both an operational response plan for cyber incidents and then having a corollary one that really focuses on the reputational side and how you're communicating both internally and externally in the event of a cyber incident. And there's crossover with the operations, of course, because part of that internal communication is making sure that the incident is escalated to the appropriate people at the appropriate time. But making sure, again, just that you kind of have a playbook that maps out the important processes and does scenario planning both on the operational and on the reputational communications side is really important. But then you want to go ahead and test those playbooks or those plans in a simulation.

Siobhan Gorman:

And it's really important that companies not relegate simulations to just something that the IT security team works on. But it really, because cybersecurity is sort of a business wide risk and a business wide issue, it's important that you do simulations at least once a year or so, with the top leadership of the company with the C-suite. And I know that there's a tendency to not do it because it's hard to schedule and it can be hard to get it on everybody's radar screens. But it's really important and the companies that work together in practice, work much better together when it comes to an actual incident.

Brian Contos:

You know, you said something interesting there, which was bringing the C suite in and I completely understand where that could add value. I'm guessing when you're dealing with a reputation response that it's not always the usual suspects that you deal with a cyber breach. Right? Are you bringing in public relations and legal and what kind of groups get involved in this process?

Siobhan Gorman:

Right. That's a great question. So, in a breach response you have a few, sort of, really key players that end up making up, in some fashion or another, the core response team. And it is often honchoed by legal, although not always. And would usually also involve certainly people who are involved from the technical side on the security front, and then it would definitely be business leads. But it would also be, if that's relevant to the incident. But then communications ends up also playing a really important role, because if there is any chance that this is a significant event that could become public, you want to make sure that you are communicating with all of your business's key stakeholders, ideally before it becomes public or before they, at least it from the media. And so, you want communication sort of working side by side with everybody, making sure that not only are you all aligned on what you're going to say, but to whom you're going to say it. And when.

Brian Contos:

Yeah, that makes perfect sense. And let's get a little bit tactical actually. Let's say, you've worked with a number of organizations in these issues so, you've been breached something malicious has occurred. What do you do or can you do anything at that point to help protect reputation or has the ship left the harbor?

Siobhan Gorman:

I guess the good news, if you will, in that circumstance is that in our experience, how you handle a breach is at least as important and, in some cases, more important, than the breach itself. So, I think that companies that are able to demonstrate a competent and confident response, I think really do fair reasonably well and sometimes can actually emerge with their reputations intact. There are a few ways that you can do that. The first is, I was just talking about stakeholders a bit earlier. The very first thing you want to do is make sure you understand who your most important stakeholders are. And as I mentioned, often your customers, depending on the company, but it also could be your employees or your business partners in some cases, the public.

Siobhan Gorman:

But you know, whoever they are, you want to make sure that you've prioritized them and you make sure that you're responsive to them. And part of that as, as I alluded to earlier, is making sure that they hear about it from you and not from somebody else. You also want to make sure that your important stakeholders know the steps that you're taking to protect their data and what they can do as well. So, as much as it is risky to talk about the details of the scope and the nature of the incident, it is not risky and it is important to talk about the steps that a company is taking to address the issue and to help their customers, or their important stakeholders to protect that data.

Siobhan Gorman:

And those are things that you can talk about and again that's what helps demonstrate that confidence. And I think, the last thing is that you do want to make sure that you aren't providing details that have a reasonable probability of changing. Because basically you don't want to say anything that you wouldn't stake your job on because you might have to, and you can ask any assortment of former CISOs and CEOs that question, but when they all of a sudden have to change their story after.

Brian Contos:

Yeah. Nobody wants to be the CISO that says we lost 100,000 customer records and then the week after, sorry, it was actually a million customer records.

Siobhan Gorman:

Exactly.

Brian Contos:

Right. A what a rough situation to be in. You know, in cybersecurity there tends to have to be a lot of education awareness and evangelism internally, especially to the C suite about the ... sometimes the needs of cybersecurity and to really educate everybody. Is that the same when it comes to this side of the house? Do you really have to

educate the corporate leaders as to what the issue is and why there does have to be a plan in place and it has to be practiced and all these things, is that something that's just more intuitive? Do they get it?

Siobhan Gorman:

I think it's hugely important. And the interesting thing is that you see this in companies of all shapes and sizes that most companies have to deal with issues and some flavor of crisis at different points in time. And there's a tendency to think that there's a certain similarity across different types of crises. That's not the case when it comes to a cyber crisis. And I think leaders need to be particularly prepared for the fact that you're really not going to know very much about what happened, who did it, what got stolen, or what broke down. At a point where you may have to start communicating about it. And it may be to business partners, it may not be publicly, but you still need to be able to demonstrate that you're on top of it even when you don't know very much. And that's a very uncomfortable place for corporate leaders to find themselves.

Siobhan Gorman:

In fact, I remember, having a quite a large conference call with a CEO and, sort of, his leadership team on ... this was shortly before they were going to go ahead and have to announce that they had a breach event. And they turned to the security consultants that they had on board and they said, "Okay, you know, so what are we going to know like the number of records?" He was asking all these specific questions and the experts came back and said, "You know, we aren't going to have that information for quite some time." And the CEO, perhaps understandably, but not particularly helpfully, launched into a rather expletive-filled tirade against the team that they needed to know more before they were going to talk about this publicly. But you know, for a variety of business reasons, they didn't really have that choice. And so, it's really important. I think for corporate leaders to kind of understand and have their expectations set in advance so that they can kind of prepare for how it is that they are going to manage a situation where uncertainty is really a that's – a

Brian Contos:

Yeah. And you know what, because it's ... as you mentioned earlier, you're pulling in legal and all these disparate organizations that maybe sometimes don't always work together. That's a very hard thing to do from a bottom up perspective unless you have that executive buy in to sort of just make sure all the gears are working together. So yeah, that makes a lot of sense. Let's talk a little bit about lessons learned. I mean there's been a significant amount of breaches in the annals of a cybersecurity history. What can we learn from companies that have taken that significant reputational hit following a breach?

Siobhan Gorman:

I think that's a great question because it's really important, when breaches don't go well very publicly, companies just sort of get dumped on. And I think that fortunately, part of the cybersecurity ethos is actually to take lessons learned from these kinds of things. That's a much, sort of more productive way that engineers tend to look at things. Although, it doesn't always happen that way in the public discussion. But I think that's really important. There are three maybe that I would point to from relatively recent examples. First is how you handle a breach is as important as the event itself. And I noted that earlier, but we really saw that with Equifax when they compounded the damage with a sloppy response.

Siobhan Gorman:

You know, I mean, among other things, they meted out a link that turned out to be a phishing site that was posing to be sort of the Equifax response webpage. But they did it from their own corporate account. They weren't sort of linked up enough to know what webpage they needed to be pointing folks to. They issued a press release that was so ridden with various errors that there was an entire slate story that was devoted just to criticizing the press release. Their CEO put out a video that ended up being really tone deaf. It seemed to be still kind of downplaying the problem and not appreciating that there were 140 some million people out there that were pretty upset about it. So I think that making sure that once you get to the point of handling it, that you really do focus on managing it well and kind of demonstrating that you're on top of it and in a really big episode, making sure that corporate leadership really demonstrates that they get it and that they're responding to it and they're addressing the issue.

Siobhan Gorman:

The second thing, I think is, you really don't want to say too much too soon, too confidently. There was a cell phone company called TalkTalk. or there is a cellphone company called TalkTalk in the UK that had a breach a few years ago. And within a couple of days the CEO came out on sort of the British equivalent of the Today Show and basically said, "Well, probably all 4 million of our customers were breached. And so, you know, take note of that. And we

received a ransom note from ISIS so we think they're behind it." Well that obviously created a fair amount of concern among their customer base and it was really unfortunate because it was totally unnecessary. It turned out that, if they had waited a couple of weeks to speak too ... speak more concretely about what happened, they would have known that it was only 150,000 of their customers and it was not ISIS. It was like a few teenagers in the UK who had done it.

Siobhan Gorman:

So, you really want to be careful because you don't want to over overstate what has happened either. But you don't want to underplay it either. And I think that, that's kind of the third point. That you want to make sure that you're calibrating your response to the nature of the event. And you do that over time because your understanding of the scope is going to evolve over time. For example, the recent breach that we saw with Capital One was kind of an odd response. They got criticized specifically for saying ... and I think this was in a press release or their letter to customers saying no bank accounts or social security numbers were breached.

Siobhan Gorman:

And then in the very next paragraph they said 140,000 social security numbers and 80,000 bank account numbers were affected. And I can see how from a company's perspective, when they're looking at a large number of records compromised that a small number seems like nothing, but to an average person, anything that has a thousand after it, is going to seem like a large number. And it's going to look like they're trying to underplay it. And so, you really have to be careful about how it is that you're describing the nature of what has happened.

Brian Contos:

Yeah. Those are all fantastic examples and some of those, like the Equifax one, I've been through tons of breaches over the last, 25 years in this space. But that's one of the only ones that stands out in my mind where I had to get on the phone with my parents and my sisters and my cousins and nephews and nieces and tell them how to go freeze your credit and how to do it with all the major credit reporting agencies.

Siobhan Gorman:

Yep**.**

Brian Contos:

And just what a personal ... that that one was very personal, I think, to a lot of people. So, like you said, being empathetic when you're the CEO of an organization like that to let people know, "Look, I know we've caused you some pain." As opposed to, "Don't worry about it." But let's ... we've talked a lot about companies, but beyond companies, where else do these breaches pose a significant reputational risk?

Siobhan Gorman:

Well, I think breaches affecting most entities probably pose a fairly significant reputational risk. I think in terms of what we're seeing today, there are probably three that I would point to as being kind of at the top of the list. The first one is elections. Obviously given the fact that we're headed into an election year and the last election cycle certainly saw considerable meddling, attempts at meddling, attempted cyber attacks, exposure of emails, and misinformation and disinformation. I think that that is an area where it's really important that those who are in charge of the different components of the election apparatus from campaigns to election officials, are doing what they can to both shore up security and also make sure that they're in a position to really maintain public trust in the system if something were to happen

Siobhan Gorman:

The second is nonprofit think tanks and they are an important one because, I'm sitting in Washington right now, but this would be true in other cities as well. They hold a lot of information, some of which is pretty sensitive. And because they are smaller organizations, oftentimes they just don't have the resources to have the level of cybersecurity that a major company or a government agency might. And yet hackers understand that they interact with important government agencies and important companies all the time. And so, they can often become targeted. And they can be seen a little bit as a weakest link that's a little bit easier place to get information.

Siobhan Gorman:

And then I think the third I would point to is universities, and that's for the same reason really. That universities are doing lots of sensitive research, they have lots of sensitive intellectual property. They have lots of data and all of

those things are really valuable to hackers. And again, I mean universities are all about openness and so it's very hard to construct truly, truly secure systems in an organization that is fundamentally trying to be open to everybody. And that's a very hard challenge for the security, the security leaders at universities. And so that's another one I think to keep an eye out for because certainly for university their reputation is quite important for their long term sustainability.

Brian Contos:

Yeah, absolutely. And Siobhan, thank you so much for that overview. I think that was really eye-opening as it relates to reputation. Maybe an area that we don't pay enough attention to from just the simple bits and bytes perspective that we might be focusing on our day-in, day-out jobs. But I have one final question I'd like to ask you and that's who is your favorite superhero or supervillain and why?

Siobhan Gorman:

You know I think I would point to Carol Danvers, also known as Captain Marvel. She's really one of those kinds of kick ass first, ask questions later kind of superheroes. And I got to say she's also very business savvy because that Captain Marvel movie, I think it grossed over $1 billion. Which is pretty impressive. So, I'm going to go with her.

Brian Contos:

Yeah. I think we'd all agree she kicked some butt. And I never thought about it, yeah, some business savviness there as well. So, nice call on that. Well, thanks so much, Siobhan, and thanks to our listeners for joining and be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.