Eye on Security

Cyber Security Through the Eyes of a Journalist

Transcript

Luke McNamara:

Welcome to another episode of the Eye on Security Podcast. I'm your host, Luke McNamara. Joining us today, we have Sean Lyngaas. Sean is CyberScoop's senior reporter, covering critical infrastructure in a range of hacking groups and activity. He was previously a freelance journalist in West Africa, where he covered everything from a presidential election in Ghana to military mutinies in the Ivory Coast for *The New York Times*. Lyngaas' reporting has also appeared in *The Washington Post*, *The Economist*, and the *BBC,* among other outlets.

Sean, welcome. It's great to have you here today.

Sean Lyngaas:

Thanks for having me, Luke.

Luke McNamara:

This is a bit of a different one for us, but I thought it would be interesting to have someone such as yourself on here to discuss and hear your perspective, in that you are covering many of the same sorts of stories and trends that parallel I think a lot of our public work here at FireEye and Mandiant, but also, in some ways, looking at this a little bit differently.

Maybe where we can start is the discussion around something that I think exists in the problem of information consumption today, signal-to-noise, and specifically, how we're making sense of threats and trends. So maybe to kind of set the scene here, I think you could make the argument that we are living in the golden age of information about cyberthreats.

You're obviously familiar with this from some of the reporting that you've been doing, but whether it's FBI indictments, Treasury sanctions, where we're getting more information around the backend organizational nature of some of these groups that maybe we just see their activity and know them by an APT and a number. You have Cyber Command releasing hashes of North Korean malware. Of course on the commercial side, you have more vendors putting out white papers, blogs, et cetera. So we have more information than ever before.

One of the questions I've been thinking through this year, is it making it harder for policymakers, for organizations, and the general public to really identify and prioritize the right threats? I know that's a big question, but how do you think about that?

Sean Lyngaas:

That's a good question. Let me just start by saying I appreciate the role reversal here, where the researcher is interviewing the journalist rather than vice versa.

It is a great question. We are inundated with a lot of noise, and our job as journalists is to be the filter and present what we think the readers, [which] should include folks like yourself and as well as a more general audience, need to see. So every day that is a challenge, because just in the last couple of weeks we've had a flurry of high-profile DoJ indictments of hackers, and that needs to be covered.

From our perspective, we always need to cover that kind of thing because it's the US government laying out evidence in the public eye of things that private security firms, like FireEye, have tracked and putting out there for people to see. So that's sort of a – I'll say authoritative, but that was a powerful statement in the news.

At the same time, we can't lose sight of all the things that we're covering leading up to the election. Right now, in terms of coverage, I basically start with election security every day. What's going on? Are there going to be social media takedowns of the Russian Internet Research Agency or some other troll farm, because we're up against the deadline with the election?

From there, we go back to what is the most interesting. I actually did a story this week related to the conflict in Azerbaijan and Armenia, not household names for our readers probably, but

we did a story because it's an old conflict that has kind of flared up again, and there is the proverbial cyber angle because someone, we don't know who – this is based on research done by Cisco Talos – where someone is conducting some espionage using a RAT, remote access trojan, against the Azerbaijani government. Now, normally would that be a story? No. It's a story because there's a conflict going on there, too.

So your question about filtering is so important. I think what I've noticed is there are more and more journalists getting into the cybersecurity space and that's really good. It just takes a while to learn the ropes and know what is news and what isn't, and who you can trust in terms of sources. There's more people – there's startups coming in. So whenever we get a white paper or something from a company we've never heard of, that is sort of on the back burner, they have to sort of prove themselves as trustworthy and we have to vet it.

So never a dull moment, but I think the relationship between journalists and security researchers has arguably never been better. The more trust that is built up over time, the better the reporting gets. So that's kind of what we rely on to navigate these things.

Our filters include analysts like yourself, people who can help us process and digest things. Sometimes when news comes out, I will, without even reading it that closely, a new threat report or something, I will fire it off to different researchers as a sort of crowd source to save time. Now, I have to do the work, too, but the filter is sort of a collective filter.

Yes, you can let more people into the circle of trust, but they sort of have to earn it. Like a company that you've never heard of, a startup that's hungry for press attention, a researcher who you don't know, they have to earn it to be part of that filter.

Luke McNamara:

Is there a role that narrative plays in this as well? Thinking to some of the comments you were making about certain things that you know are going to be of interest, so certainly if APT28 does something new or there's a new story around Sandworm, those are things that are, by the very nature of what's been discussed about them in the past and what we know about their activity, almost certainly to be of universal interest.

Then you have something, for example, like ransomware, where it's not a new story in terms of the activity, the capability, but the continued developments in that space have really stood out this year and have really been building I think from previous years. But then you have a situation like you mentioned, Azerbaijan, a conflict maybe that people aren't as familiar with, but potentially the chance to see emerging threat actors or capabilities that historically we may not see a whole lot of.

So you have various, I guess, things that kind of balance where some of these topics you know are going to be of interest, because there's a certain narrative around it. How do you think about that or how does that factor into, again, the topic selection and maybe how you choose to approach writing about something or the way in which you cover it?

Sean Lyngaas:

We have a body of reporting out there. Our publication has been around a few years now, and sometimes I forget some of the stories I've written because we write so much. But there are certain narratives that are sort of established with ransomware, for example, actors targeting – to borrow someone else's phrase, it's a target rich but resource poor environment, state and local governments and healthcare sector.

That was already existing, but now we have the Covid-19 pandemic and all that gets exacerbated. That's an example of an existing problem that you layer on top with new information about what's going on in the world.

So when you're approaching a story like that, you have to ask yourself, "What am I adding to what we already know?" A report about a given threat actor is not news in and of itself. That's what differentiates news from research. A new malware variant could be very interesting indeed and our readers are technical, so our threshold for writing about that is not hugely high, but it still has to tell us something we don't know already. We're not going to use platitudes like, "Threat actors are always evolving," and this or that that you see in a lot of marketing, because that's not telling you something new.

Now the challenge, Luke, a lot of times is to tell personal stories. In cybersecurity, the human angle is sometimes a bit elusive because we're talking about ones and zeros so much, but any time we can do profiles of people and tell really compelling stories, that's journalism, but it's very difficult sometimes in cybersecurity.

We recently did a profile of a – he's actually an immigrant from the former Soviet Union and Azerbaijan. He's a lawyer based in New York, who my colleague, Jeff Stone, profiled. He happens to represent many of the high-profile accused Russian, alleged, cyber criminals. Jeff spent months with him, talking with him about his personal life, his backstory, how he got to America, and then bringing that to life in a feature story.

Taking time out of our stress of the news cycle to do something like that is really important, because people really want to read that. People who aren't in the cyber industry are like, "Wow. That's really interesting." I think we could have had Jeff, my colleague, on national television talking about that story because it's that interesting.

So that's the challenge in balancing those things. We have a technical audience, but we also want to tell stories and I'm always looking for that. It's about finding the time to do that, while also keeping up with the flood of the information that's coming out.

Luke McNamara:

This year, where we've had so much coverage around Chinese threat actors and the indictments around that, the theft of intellectual property, obviously right now in the middle of election season, the nexus between that and security is very much of interest. But outside, where there are these larger news cycles driving particular interests, are there particular stories or aspects of this space that you feel like are maybe underreported or underrepresented in the general kind of awareness of what's going on in threat activity or cybersecurity as a whole?

Sean Lyngaas:

I think so. It's challenging, too, because the APT reporting is always going to be sexy and of interest to readers. But is that necessarily the thing that your average IT administrator needs to know about to arm him or herself to defend their networks? No, but it's easier to write about and it's more compelling.

So there are under-told stories, but, again, we're not writing manuals for IT security. We're writing news stories.

That said, there are certainly other stories that I think could get more attention. We've been doing more reporting on stalkerware, spyware on your phone that's been linked with spousal abuse and that sort of thing. I think that didn't get nearly enough attention until the last several months. The EFF and other organizations have brought it to the forefront. Again, that's an example of a type of malware that gets overlooked, because I think a lot of vendors are hunting for the next big bad APT, where protecting the average person with things on there is a little bit more relevant in some cases.

There are always angles that we're overlooking because we can't catch them all. That's why I routinely put out the generic call for, "Talk to me. What are you seeing people in the industry?" kind of thing. It's not a solicitation to tell me about your new product, because we don't really write about products at all, but I'm always checking in with sources and saying, "What's out there?"

If you have the visibility or if you have some visibility, I'm sitting here at home, especially right now during the pandemic. I don't have a platform, telemetry. I don't have things that I'm just looking at in terms of indicators all the time. That's all on the other side of the transom.

So it's a constant need to ask people what they're seeing and being actually quite annoying about it. I mean I can do it with people if you have a good relationship, like, "Hey, checking in again. I know I'm not the only thing going on in your world, but I always need ideas." So that's kind of how I approach it, just being incessantly inquisitive with people.

Luke McNamara:

I think that's part of what I was really interested and looking forward to with this discussion around is everyone has a different aperture and visibility in this space, and the things that they are focused on highlighting and drawing attention to are going to vary as well, whether you're talking about the media or academia, the commercial sector, the public sector. One of the areas that in particular I'm interested in your thoughts, and maybe what it helps inform and tell us about how this space is evolving on the whole, is an area where you guys actually recently just put out a piece this week on it, about Bahamut and the sort of space of hacker for hire, cyber mercenaries, surveillance technology, however you want to frame that.

But outside the larger discussion around the big four and countries like Vietnam with APT32 and developing their organic capability, what do you think we're seeing in some of the other

parts of the world, where you're seeing these capabilities being exported and these hacker for hire groups increasingly seem to be popping up more in the news?

Sean Lyngaas:

Yeah. I think with the hackers for hire, the money is usually so good that it breeds that sort of market for that. I think these tools that are out there – you're familiar with the Project Raven reporting that my former colleague, Chris Bing, has done with others at Reuters on how the UAE spun up their capabilities.

I think it's just a function of economics. The tools are out there. People leaving intelligence agencies and just the amount of money that can be thrown at them to develop this stuff. I think the market is only going to get bigger for that.

I think the challenge is shining a light on some of these vendors who have been very aggressive in protecting their image and fighting back. NSO Group is the obvious example. They hired a very prominent PR firm in the US and have been talking about some of their reported humanitarian work with tracking different humanitarian issues, their technology being used for good. We don't necessarily get a full picture of what's going on.

That applies to a lot of other firms. NSO Group is just the easiest example. They have done more interviews with journalists, and they are putting more things in the public eye, but the need to expose more and more of those tools I think is something on every cybersecurity reporter's mind. It's one of the more interesting things out there to investigate. I think, like I said, the market is going to just keep going and propelling that.

We could dedicate our entire time to investigating those firms and the way those tools proliferate. Also, if you look at some APTs, there's a bit of mingling, rubbing shoulders with these 0-Day venders, too. I've done recent reporting on that in terms of – I think it was a new threat actor that ESET published on last week. It's espionage targeting Eastern Europe. Okay. That sounds like government-on-government spying.

Also included in the report was the likelihood that this group was sharing an exploit vendor with our hotel, the APT out of supposedly, allegedly, possibly out of South Korea. So it's a very murky world out there in terms of spies and co-developers who are offering their services.

That was also a very human angle, too. Talk about NSO Group spyware and Hacking Team's spyware, other tools that have been used, allegedly, on human rights activists and others. People say, "Well, that's a story that is hugely important, and I can relate to that more than I can relate to stories about various APTs doing their thing." Espionage is espionage, but when it involved tracking dissidents and people that end up with serious, physical, real-world consequences, that gets people drawn in. That gets policymakers paying attention. There are senators who have responded to reporting on surveillance tools like that.

So that stuff is more interesting, and it's an underground bazaar of tools. I really encourage more researchers as well as journalists to investigate that, because we need each other in shining a light on that economy.

Luke McNamara:

I think it's particularly interesting thinking about it from – and I know your background is in international relations and that space. Looking at that convergence of these capabilities and the proliferation of these capabilities with what some would call the increasing vulcanization of the Internet and technologies, the sort of discussion we see around 5G technology or whether or not certain tech companies, because of where they're headquartered, can do business in certain parts of the world or not.

So I think it's interesting to kind of think about not just – the space of emerging threat actors is always one of the more interesting ones to be, because you get to really see for the first time how a particular state actor builds a capability or buys an off-the-shelf capability or is using some service. You see the sort of revelation of their national interest and collection priorities are as more information comes out around that.

So I think that will be an interesting space to look at, certain companies that are offering these sorts of services or they're in the exploit for sale business. Are there certain places where they will be allowed to do business by the country that they operate out of? Will there be certain places where you see an interest in buying those sorts of capabilities, where there's a skillset, people coming out of the military and government in particular countries that have a certain skillset?

So I think the convergence of all those things, once you layer on the vulcanization piece, will be very interesting to look at.

Sean Lyngaas:

Absolutely. I think the tools are going to be available to certain buyers in certain regions, because of whether it's US sanctions or just the general, like you said, vulcanization, segmentation of where goods are bought. It's going to be accentuated by some of these other trends that we're talking about.

Luke McNamara:

Moving on to disinformation, because it's an election year and election security is a top priority, we can't avoid that as a particular topic. That's really one that I think in many ways, although certainly there's applicability in other different spaces in its usage, has become synonymous with election security, the discussion around disinformation.

From the perspective of working in journalism and covering disinformation or how you've seen it covered, what are some of the specific difficulties in discussing that compared to some of the other types of cyberthreat activity? I guess in particular, and this is a little bit of a leading question, obviously, the challenge in reporting something, but not amplifying it. How do you approach that?

Sean Lyngaas:

We think about that all the time. Look, we're not *The New York Times.* We don't have millions and millions of viewers, but any good journalist takes the trade craft the same way, if you have five viewers or five million.

The lessons about not amplifying, people are heeding – 2016 was a bruising experience. I wasn't here covering election security then. I was in Africa at the time, taking a break from cybersecurity. But I think the national news outlets learned from the covering of Wikileaks, and how that just did the Russian's bidding for them in proliferating reporting on that a bit too breathlessly.

Right now, we're in a very tense situation where, like you said, the threat to elections is really disinformation, I think. I mean not to say that voter registration databases are not an issue that's being addressed at the state and federal level in terms of protections, but it's perception on how people – we don't want to amplify anyone's fear or anything. I have refrained from covering certain things in the last couple months because I worry about being a vehicle for hyper-paranoia.

There are some very good election security exercises that go on in the private sector, but they often deal with sensational scenarios. If you write a story a couple months from the election about explosions of voting booths and fictious scenarios where people are red teaming it out, where they're just trying to improve security, but it makes it seem like the world is on fire, that's not a good thing.

I think right now among journalists, there's sort of a commitment among people that cover election security to take that extra couple breaths and pause before thinking about covering something. There was a good example a few weeks ago of a report in an at least semi-independent Russian news outlet. Now, that's not an oxymoron. There are a couple out there, a news outlet called *Kommersant* that ran a report suggesting that there was hacked voter registration data on underground forums, current data, multiple states.

It was portrayed as a big story and a couple prominent media figures in the US tweeted it out, one in particular as if it was a five-alarm fire. We all looked into it, but we did so behind the scenes before saying anything. If I were to tweet out, "Oh god, look at this, hacked data, not good." Someone who doesn't even follow me, with 500,000 followers, amplifies that and all of a sudden we've got a cascading thing that gets picked up. Sometimes national media outlets run with that way too quickly, and we're down the path towards repeating 2016's mistakes.

So in this case, many of us verified it, vetted it behind the scenes and realized that, no, that data was already publicly available. It was not newly obtained data. We got statements from federal and local officials. So my headline on that story was, "No, Michigan voter data was not hacked," because the Michigan Secretary of State came out against that story very vociferously.

That felt like a drill. Maybe we'll have another one between now and then. If you look at Facebook's latest IRA, Internet Research Agency takedown, there are some quotes in there

from the head of security policy at Facebook saying, “Well, we know how quickly this can pivot to hack or leak,” or something like that, “so we’re trying to squash them right now.”

So we’re all kind of on guard for an eleventh hour dumping of material. It will be interesting to see a) if that happens, and b) who will show restraint and who will take the bait.

Luke McNamara:

One of the areas where I think there has been maybe less discussion around disinformation – certainly we’ve seen kind of an explosion in the overall conversation around disinformation from many different angles since 2016, but one of the areas where I think it’s not been explored as much and, in all fairness, I think it’s probably the hardest question to answer, certainly when we think about it though from a cybersecurity standpoint, the big question across any activity we’re talking about, what it is, is impact. What is the impact from this? What did this succeed and result in doing?

That’s true if we’re talking about an intrusion into a power plant. The impact around disinformation is one – again, in part because it is so difficult to ascertain. Maybe there are metrics that you can kind of capture and look at from how many people viewed a post, or how many people reshared a piece of information that was part of an IO campaign in a network pushing disinformation.

But the actual ascertaining of impact from these sorts of events, that seems to be something much, much more challenges. How do you think about that in the coverage of these sorts of networks that, again, we continue to see, we see from an even wider group of threat actors than in 2016, and we’ll probably see more and more enter this space? How do you think about the impact piece of this?

Sean Lyngaas:

Impact is so important and sometimes it is difficult to ascertain. I have to put lines in stories here and there saying it’s unclear. You always ask the researcher or the government official, “Who do you think is behind this activity?” “Oh, we don’t know,” or, “We don’t want to say.” Okay. Well, we have to tell the reader that we don’t know, or they don’t know or they don’t want to say.

Then it's a similar thing with impact. There are certainly metrics you can use in measuring engagements online, but it's hard to know the full scope of an operation and where it begins or ends.

I think in terms of not amplifying and covering something that – it's important to note intent also. Just because it didn't have a big impact, the intent of the actor behind it is revealing and could be news in and of itself. Yesterday, as you're aware, the Department of Justice announced the seizure of 92, I think it was, domain names allegedly used by Iran's IRGC as part of disinformation campaign. Only four of those domains were focused on a US audience.

But, and I haven't looked at this one closely, if you're writing that news story, what kind of engagement did those posts get? Then you would go to folks that study this stuff, places like Graphika or the DFRLab, Atlantic Council. Again, it's leaning on people with visibility.

One other thing I would say, Luke, about this not amplifying is people are learning a lot of this covering the Trump administration, the president in particular. Yes, he's the most powerful person in the world and you're covering him. He's a news maker, but to not amplify disinformation or misinformation coming from him, especially in the election season.

You start at the top of the story with these are the facts with voting by mail, and how there's miniscule evidence of fraud and that kind of thing. Further down in the story, maybe you mention what Trump said incorrectly about this issue, and then you add another check on that. That's from one of the best journalism minds that I know, in terms of just fundamentals, Margaret Sullivan of *The Washington Post*. She's a media columnist and she has her eye on the media and how journalists are covering things, and how they're coming up short or doing well, but that's what she said the other day in terms of structuring story.

The headline is so important, too. You don't start with, "Mail-in Ballots are a Rife Opportunity for Fraud, Trump Says." You say, "Despite Scant Evidence of Said Fraud, Here's …" You structure it in a way where you lead with the fact, and then you follow with the claim that's being made.

Actually, at this point, that's not a great example because I don't even know if people should be covering his individual comments every day about fraud. That is the biggest challenge right now. Domestic misinformation with the election is the biggest challenge right now. We've

talked for years about the different foreign actors that were spinning up to interfere in the 2020 election, but calls coming from inside the house right now with challenges in putting factual information in front of people about the integrity of the election, how voting by mail is secure.

Mail-in voting is not the first story I think of when I think of CyberScoop because it's not network security or anything like that, but it is, broadly speaking, a security story, a cybersecurity story. So we put out an explainer of the history of voting by mail, the checks on it that election officials do. Cases of suspected fraud are exceptionally rare.

All those things are very important to keep in mind. Again, we don't have the biggest platform in the world, but right now, the election is the number one issue on everyone's mind, and yes, there's a security angle. So that's one thing that we put out the other day.

Luke McNamara:

Moving away from just the election, where do you think the public discussion around disinformation goes from here? So in terms of how this has kind of evolved to-date and –

Sean Lyngaas:

Yeah. I think you could go in a couple different directions with that. The outsourcing of this kind of thing, we saw after 2016 the Internet Research Agency was sort of outsourcing a lot of this stuff. There was an investigation by CNN into some of those operations in Africa, where they were paying people on the ground here.

The more recent takedowns on the platforms involving IRA have been cases of paying, dangling money in front of freelance journalists who are particularly hard hit by Covid and saying, "Hey, will you write an article about liberal politics for $200.00?" "Sure." It turns out your editor is not who he says he is.

But from there, I think there is supply and demand for this kind of stuff. So any mature discussion of disinformation has to take stock of the fact that US, American society is still ripe for being exploited by disinformation, and not being able to process – you talk about the erosion of traditional media, quote/unquote, and the immergence of partisan news outlets that are one side or the other. I think that has a lot to do with people's susceptibility to this sort of thing.

Luke McNamara:

Yeah. I want to spend some time, a little bit, I'm interested in what you think of – and this actually is less of a cyber-related question, but from the standpoint of how you think the future of media and consuming news will evolve. So thinking about this maybe from an analog standpoint of how I've seen, in a short period of time, the ways that folks are understanding and consuming intelligence in terms of what are the use cases for it, how they want to consume it, what it needs to look like from either the raw data to a finished piece of intel. All of that has kind of evolved and changed, in part as organizations' maturity has evolved.

But I wonder if there's something kind of similar with news and, again, getting back to this question of sense making and all these narratives and events and incidents taking place for organizations, for individuals, for the general public that's trying to understand that and how they're looking at consumed news. How do you see that evolving going forward in the future?

Sean Lyngaas:

My first reaction to that question is that some news outlets have kind of enjoyed the resurgence in terms of subscribers pre-Covid. People were paying for news again. There was more demand there. With Covid, so much decimation to various sectors on the economy, the local news aspect of that was particularly – I mean, from our perspective, as a journalist watching that, it was pretty heartbreaking because you had some long-time papers that were doing good work in their local communities closed.

This is all related, our susceptibility to disinformation, the dearth of what people consider reliable sources out there. When local papers shutter and aren't serving the community anymore, people go online to whatever they consider that conforms to their political views and they start to – it's almost putting it a little too strongly, but a radicalization process.

So any new, creative ideas about sustaining independent journalism. You just ask people to pay for the product. If you want a good service of anything, you pay a little bit of money for it.

I don't have any wildly innovative ideas because, frankly, I'm in the trenches every day. Certain people think about this more than I do. I had a friend from graduate school who is taking a break from his previous career and said, "I'm going to think about how to shape up the news industry." I said, "Great. Let me know when you figure it out."

For a while, there's this – do we rely on philanthropists, a very wealthy philanthropist to come and buy your paper, and have a hands-off approach and not interfere? Jeff Bezos bought *The Post* and that was a great, huge injection of cash I'm sure, and that's great stability, but not everybody can have that mogul come in and buy it and not be involved in it.

So I think about this a lot personally, but not in terms of how do we solve it collectively. It's something that is hugely important. I think our attention spans are shrinking as a result of social media, and that's just the way things are going. I have to be on Twitter an inordinate amount of time for job because something might break. I might get a notification and all of a sudden I have to write something. That's the trade-off we're in.

I think we always run the risk of underestimating how smart people are and their willingness to consume and pay for news. I'm sure there are silver linings here and there. Newspapers have closed during the pandemic, but other ventures have opened up. I'm just optimistic that there are people out there, plenty of people out there who are like me, who like to read well-reported things, who rely on it to make decisions.

That's always going to be the case, regardless of how polluted different parts of the ecosystem have gotten with partisan noise and disinformation. You've got to stay optimistic about people's intelligence, because there are a lot of brilliant people out there who still want to see good news.

Luke McNamara:

Yeah. Again, consider from the standpoint of very easy to become swamped with the amount of information out there, even the amount of intelligence out there as we began the conversation.

In terms of closing and wrapping this up, I'm curious what your thoughts are around trends. We've obviously discussed a lot that you've been following closely, but it's hard to believe we're almost at the end of this year. Going into next year, what are some of the trends that you think are especially notable for listeners to be following?

Sean Lyngaas:

Things I'm spending a lot of time reporting on right now are healthcare and cybersecurity issues in healthcare. In the last couple of weeks, we've seen eye-opening ransomware incidents at Universal Health Services, one of the biggest providers in the US. Then there have been other instances. So I'm increasingly thinking about the intersection of cybersecurity and health and safety. I don't imagine that's anything that's going to subside in 2021.

Other trends, one thing that we follow a lot with this US administration is their embrace of more muscular offensive cyber capabilities, at least as much as they talk about it. Cyber Command is over a decade old. Under its current leadership, it's really talking a lot about taking decisive action and that's really interesting to follow, and the reactions it has for whether it's norms in cyberspace or any blowback that might happen in the private sector with the US going on the offense more. That is a trend we're following a lot.

We just did a story this week. I believe it was this week. Sometimes it's hard to keep track of the days. But the Treasury Department is warning about people potentially violating sanctions by paying ransoms. So that's really interesting.

The ransomware ecosystem will never stop as a storyline. Who's facilitating payments? Who is backing up their data? Who is maybe a state affiliated actor masquerading as a criminal actor to the ransomware, that you conduct a ransomware operation? Some of them are very hard to prove, obviously, so they never end up being stories, but we will never stop investigating who might be behind something.

It's really funny, Luke, as you're well aware, how people a couple years ago used to talk about how hard attribution is, and it's still hard, but not as much anymore. Attribution, sometimes researchers get annoyed at journalists for asking, "Who did this?" Of course we're going to ask that because people and names and identities are part of storytelling. So if you know who it is, it's that much more interesting, and you can divine their motivations and that kind of thing.

So I think a lot about, any time there is an incident, "Who did this?" A lot of times we can't say who it is because we don't know or we don't have enough evidence, but that will never stop being a thing that we revisit, revisiting major breaches that happened.

I guarantee there will be more announcement in the not too distant future about enforcement actions from the government. I mean I don't have any hard – you know, I'm just saying the way things have been going, there's going to be a lot of activity where incidents from the past – at the beginning of the year, I think it was February, we'll just say near the beginning of the year, seemingly out of the blue, for us anyway, the DoJ blamed the People's Liberation Army officers in China for the Equifax hack. I hadn't been thinking about the Equifax hack that much. It was years old.

So there are these kind of cold cases in some ways that some of them you never hear about them again. Some of them are still being investigated and then get unearthed unexpected. So that's the kind of thing that really excites me about this field. More than a lot of others, there's a long memory and the data doesn't lie. If people are able to stitch things together, you never know what's going to break news in the next day.

So in terms of 2021 trends, I would say protecting hospitals and healthcare critical infrastructure from criminal actors. Nation states as well, but right now, a lot of what I'm seeing and thinking about is not state affiliated in terms of ransomware that kind of thing.

You could also talk about the proverbial skill shortage in cybersecurity and that kind of thing, how we reimagine how these kinds of positions can be filled. I'm sure FireEye has several people who are not traditional, don't have 17 different certifications, and they're not software engineers necessarily. I'm sure some people are, but it's people with BAs in philosophy or international relations, who are critical thinkers, who are able to do the threat hunting.

That's true for – industries increasingly hire journalists to help, to be analysts or look at problems differently. People tend to sort of get drowsy. When you're a journalist, you talk about, "Well, let's do a story on the workforce." Now, that sounds boring on its face, but it can be interesting.

I've done some stories over the years on veterans, people coming back from war, going into the cybersecurity industry and using their talents in that way, and how many opportunities there have been and continue to be in that space for them, and that's really interesting. Again, that gets back to the people side of the equation.

So those are some of the things I've got my eye on. I'm sure there will be more if you ask me in a couple hours or next week.

Luke McNamara:

Yeah. To the point about the kind of people-centric approach and attribution alongside the impact question of, okay, there was a breach here or there was a disinformation network uncovered, what was the actual resulting impact from that? The who is behind that is always going to be one of those foundational questions that I think as an ecosystem we've only gotten better at answering.

Sean Lyngaas:

Indeed.

Luke McNamara:

And in part, again, to go back to when we began this discussion, the fact that I think you've seen more of a willingness from government organizations to tip their hand through indictments and sanctions to give us a window into that, and that has certainly informed, I think, our understanding of what those relationships look like, who those individuals look like, behind something that can be a very banal operation and set of activity. So definitely something I think that across all these different topic areas that we've discussed here, will be interesting to follow going into next year.

For folks that are interested in it and following along with your work, where can they follow you on Twitter and at CyberScoop?

Sean Lyngaas:

We're at CyberScoop.com. We have a free newsletter every day. I know everyone has got a newsletter, but ours is really cool. I'm on Twitter as well. My last name is a little tricky, but if you just Google Sean and CyberScoop, you'll be able to find me. I'm on Twitter @Snlyngaas.

Luke McNamara:

Excellent. Sean, thank you for coming on today. Definitely, everyone, go check him out and check out the great writing from the folks over at CyberScoop.

Sean Lyngaas:

I really appreciate it, Luke. It was great talking with you.