"The adversaries are the ones that benefit when we don't talk about threat information, when we get caught up in mistrust or red tape and all of the things that block open communication. The more open we can be, the more efficient we can be in the transfer of knowledge. One company can't solve the problem. One government can't solve the problem. We need to come together in order to combat this. And the only people who benefit from keeping this to ourselves is the adversary."

MARCH 9, 2020

Insightful Intelligence

Presenter: Sandra Joyce

Summary

The history of human warfare tells us that the recipe for victory is often a concoction of technology, strategy, and intelligence. Today's guest, Sandra Joyce, is the SVP of FireEye, the world's largest non-government cyber intelligence organization. She and Brian discuss significant trends, what to consider before publishing hard-earned intel, and the cleverest adversary tactics to date

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 Sandra Joyce. Welcome to the podcast, Sandra.

Sandra Joyce:

Thank you for having me.

Brian Contos:

Sandra, I've got a number of things that I'd like to ask you today, but before we jump in, could you give our listeners a bit of background about you and sort of the path that you took that led to, you know, what it is you're working on today?

Sandra Joyce:

Of course. So, I'm senior vice president at FireEye, a cybersecurity company, and I lead the cyber intelligence organization. And I've been doing that for the last about two and a half years. I've been at FireEye for about four years.

Sandra Joyce:

And the path to cybersecurity for me came by way of the intelligence community. So, I've been in the intelligence career field for about 21 years, some of that as a Air Force reservist, some of that as a federal contractor, and really came to this space out of, you know, post-9/11, a lot of counter-terrorism was the mission.

Sandra Joyce:

And as that was sort of, you know, running its course, what I was observing was that cyber activities started to go from being the plan C or plan D of nation states, to the plan A. And a lot of the activity that was happening on the global stage really was happening in the cyber realm. And I made an intentional shift in my career at that point to get educated, do some studying in cyber intelligence, and made that shift over a couple of years and came to FireEye and started to lead the cyber intelligence organization here.

Brian Contos:

Wow. What an interesting background. And I know there's some people that might not be aware of this, but at FireEye, it's actually the world's largest non-government cyber intelligence organization for which you run. What's it like running the world's largest non-government cyber intelligence organization?

Sandra Joyce:

Well, it can be very fascinating. So when I started out in intelligence, you know, I was at Goodfellow Air Force Base and I was learning about intelligence, and back then, it was everything was classified and it was valuable because it was rare.

Sandra Joyce:

And you know, that has changed. You would have really shocked me at that point if you would have told me that in, you know, in 2019, information was commoditized to the point where you could have an intelligence business that's gaining insights, processing data and information, and putting it out as insights on threat activity that was outside the government realm, that non-classified information was going to be as valuable, or even in some cases, more valuable about the cyber domain.

Sandra Joyce:

So, it's a fascinating shift in intelligence in general and a fascinating job because, you know, from my perspective we are looking at some of the tip of the sphere activity that is driving global events. So,fascinating is really the word that I would use to describe this job.

Brian Contos:

Sometimes are you watching the news or having conversations with people outside your business unit, or even outside our field, and you're thinking, "Oh, I kind of know some of the backstory to that," or you know, you have windows into that situation that perhaps the average person doesn't. Does that happen?

Sandra Joyce:

It does, and we can't always talk about it for contractual reasons. For example, a lot of the information that we get comes from Mandiant Investigations. And so what we know from the Mandiant Investigations is the latest, you know, tactics, techniques and procedures that some of the most egregious cyber actors are using, and we know a lot about what they're doing. And because intelligence really is about getting that geopolitical backdrop to understand why those things are happening and what's likely to happen next, it puts us in a position to really have a really good insight.

Sandra Joyce:

Because it's not just about maybe the activity that's happening at that one site, but it's also the activity that we're seeing as a pattern. And we can say, "Well, there is an isolated incident that might be hitting the news, but we know it's part of a broader effort by this nation state to achieve its strategic goals."

Sandra Joyce:

So, it's information that we we don't hold to ourselves. We definitely have to anonymize, you know, to protect our clients and their private information, but we put those insights into our intelligence subscriptions so that our customers can benefit from it. And then under some circumstances, we'll actually put out public information when it meets a certain threshold.

Brian Contos:

Sure, sure. Well, you know, your business unit, if you will, relies on the production of intelligence, not just raw data, but actual intelligence. What's the hardest part of running a group [where] that's your goal, actually generating this rich, usable intel?

Sandra Joyce:

You know, I'll answer that question just by backing up just a little bit. So, when people think of intelligence out in the world, they tend to think of things like James Bond, right? And they think of things that are more on the Hollywood side of things. And you know, the real reality is that intelligence is a career field and Tradecraft about using structured analytical techniques, right? It's about aggregating data and information, processing, analyzing it, and then putting those insights out in a usable way so that somebody can make a decision on the other end.

Sandra Joyce:

So, this was incubated. So, the intelligence incubated on the military side for military purposes, but it is very transferable to solve business questions and answer business risk questions as well. So, what it's like is there's a component of it that is very authentically based in the traditional intelligence processes and practices, but with a commercial motivator to say that not only does this have to be good quality intelligence, good structured analytical techniques, good Tradecraft, but it has to solve a business problem. It has to solve a security problem on the commercial side.

Sandra Joyce:

So, that's, I would say, the best way to characterize how we view what we're doing here at a FireEye Intel.

Brian Contos:

Yeah, no, that makes a lot of sense. It can't just be intelligence for the sake of intelligence, it has to have some type of value outside of that group and-

Sandra Joyce:

That's right.

Brian Contos:

Yeah, that makes good sense. You know, let's get a little bit more specific. I want to talk about APT41, and you've recently released some information about this. It's a China-based threat actor for those on the podcast that aren't familiar. But what I'm wondering about this and other similar threat actor groups is, you know, what kind of considerations do you have to go through before publishing this type of intelligence and taking it public, especially when it has to do with a, you know, a nation state actor?

Sandra Joyce:

Well first and foremost, the information that we have and the intelligence that we create needs to be beneficial to the global security community. And in the case of APT41, we've been watching this group for years act relentlessly, not just to carry out espionage missions for the Chinese state, but also then they're hackers for hire at night. And we can specifically see them, you know, using some of the tools that they use to carry out espionage for then a commercial purpose or, you know, financial gain after hours.

Sandra Joyce:

So, there was a fascinating threat actor. And the considerations that we go through are, you know, we need to be able to have enough evidence, irrefutable evidence, and something that can stand on its own. If we were to ever be, you know, put under any kind of scrutiny, whether that's legal scrutiny or any other, you know, magnifying glass that gets put on our stuff.

Sandra Joyce:

And so with that, you know, we have the highest standards and we always have a lot more evidence than we need to establish this kind of attribution. This is really hard work. There are many, many groups spending countless hours to make this type of analysis happen. We have clusters of activity that we track and have to be very careful that we are clustering the right activity with the right threat actor.

Sandra Joyce:

And frankly, they use techniques to try to obfuscate their activities. They take steps to try to hide their activities as well. So, we need to not just be smart about the evidence that's prevented, but we also have to be looking out for things like false flags, redirections and all the things that very sophisticated groups do in order to be undetected.

Brian Contos:

Yeah. You know, it's interesting, I first heard the term false flags used in this realm a few years back, and somebody was telling me, if you find the area of the world where there's a high volume of cyber crime, for example, and there's a lot of malicious activity, it's known to be a hotbed for that, it's really a great place to sneak in and do some real work maybe [crosstalk 00:09:39].

Sandra Joyce:

That's right.

Brian Contos:

Because it's under that cloud. You mentioned something about, you know, there might be some actors there that are, you know, nation state actors by day, with political motivation and cyber criminals by night. And I have a question about that as it relates to safe harbor.

Brian Contos:

So, when I think of safe harbor, my mind, for whatever reason, goes back to like the pirates of the Caribbean, back in the late 1600s. Not Johnny Depp, but the real pirates, and this idea that you had all these pirates, and they would hang out on the Caribbean basically, and they were allowed to do whatever it is pirates do, buried treasure, make maps, carve peg legs. I don't know what pirates like to do, but doing pirate stuff. And they had impunity and they could hang out there and do all their pirate stuff. But what they were told is, "Look, you can, you can be here. You're

safe. No one's going to do anything. But if the Spanish come by, it'd be really great if you guys went out there and blew them up and kept them away from us." And that was sort of the trade off.

Brian Contos:

Are we seeing that happening in the cyber world? Like hack all you want, do all the stuff you want to do, we're not going to touch you, but you know what? We're going to call upon you every now and again for some political stuff we need done, or some military assistance or something that's more government-focused. Is that a reality? Is that something [crosstalk 00:10:58]?

Sandra Joyce:

You know, I think what you were referring to with the pirate analogy was the letter of marque, right? Which was the authority given to raiders or to merchant ships to be able to carry out a country's mission when they found themselves in the position to do so.

Brian Contos:

Sure.

Sandra Joyce:

What we see from the point of view of threat actors is they will often use, for lack of a better word, contractors, right? So, they will find additional work that can be done. And there certainly are reasons to do that, that look a lot like the reasons why our government uses contractors.

Sandra Joyce:

But the interesting thing in the cyber domain is, sometimes using contractors in a way that can provide distance from the original sort of hand to the action, is that you are creating distance and obfuscating the original activity. So in that way, you know, threat actors will use this in order to put distance and also to try to muddy the waters as to say, "Well, it wasn't us, it was somebody who is a patriotic hacker," or something like that. So that one thing that we've observed.

Brian Contos:

Sure. Sure. So, I had this, as you were going through this, I started thinking, you know, you're the head of the world's largest non-government cyber intelligence organization. You see a lot of stuff.

Sandra Joyce:

I do. That is true.

Brian Contos:

And kind of assume some of that stuff is pretty strange. Is there anything that you can share with us, anonymized or whatever, about maybe some interesting or strange things you discovered on the cyber intelligence side?

Sandra Joyce:

Oh. So many. So many. You know, I think that to say cyber is strange is the understatement of the universe probably at this point. I would say recently, I found absolutely fascinating and, yes, very strange, some of the work we're doing tracking Iranian influence operations.

Sandra Joyce:

In this case, we actually saw Iranian actors who were impersonating political candidates in the United States pretending to be from Texas, getting their letters published in major newspapers online under the guise of being, you know, concerned American citizens, and then even getting linked to interviews that they were sponsoring where the person conducting the interview was always off camera. And this is being sponsored by the same sort of social media network that's putting out the influence operation.

Sandra Joyce:

And with that, it just seemed like a very, you know, complicated set of influence operations that I found, personally, to be very fascinating, but also very disconcerting that that's the level of effort that some of the adversaries are using to try to influence the American populace directly.

Sandra Joyce:

So, if we, you know, if we take that in, it's definitely in the realm of strange, but it's also in the realm of this is the extent to which threat actors are now going. It's not just the same activity they were doing even five years ago, they continue to amaze us with some of the techniques that they're using.

Brian Contos:

Yeah. I mean, that's super scary, right? We're talking about basically influencing in, probably, a pretty rapid way, the democratic process, right? And the way that you influence people and the way social media is designed. You know, you connect to one person, that connects to a hundred, which connects to a thousand. It's such a powerful weapon and it's not a what if, you know, it's already happened. It's already being used as you just said. That's probably its own podcast actually, or a few of them.

Brian Contos:

So, scary stuff, strange stuff for sure, but what are some of the current trends that you're seeing in the cyber cyber landscape? What's happening?

Sandra Joyce:

So, right now, what we're seeing is a rise in ransomware attacks that are going after state, local municipalities, that they're finding some of these groups don't have the cybersecurity controls let's say of the federal space or of enterprise companies, and they're really taking advantage of that.

Sandra Joyce:

Another thing that we've been seeing is, in the realm of ransomware, this shift towards post compromise, very deliberate targeting. So, you know, we will watch, for example, in the underground, somebody will say, "Well I have access to this organization." And someone else will say, "Well I have this ransomware that I want to use." And they will actually go in together and do a post compromise ransomware deployment, so they can get deeper in the organization, tie up a lot more sensitive systems that were, you know, very carefully mapped out. So not this sort of spray and pray commodity type thing, but a really deliberate movement towards a company.

Sandra Joyce:

And at that point, what that was doing was also raising the ransomware amounts, the amounts that they were demanding from these groups. And that's in the category of ransomware, so trends that we're seeing.

Sandra Joyce:

Another one is just the tendency for some threat actors to take the destructive approach. So even a few years ago, I would say that there was a real knowledge gap between what a threat actor could do and how much destruction they could actually carry out. We published on Triton malware, where we were watching threat actors that, in our view, probably accidentally deployed into a ICS facility shutting down the facility. And we don't think that that was even an intentional thing. And as many people know who look at these types of facilities, that kind of action can really be a dangerous act, where these things tend to need to have, you know, a lot of really carefully coordinated, instrumented, methodical processes to shut down safely. And in this case, the threat right actor was quite reckless.

Sandra Joyce:

And so what we're seeing is an increase in recklessness over time, the willingness to take more risk, and a lot of that is tied to nation state activity. So, we actually attributed part of the Triton malware piece to a Russian government center, and that's frightening in in one way to think that nation states are taking reckless steps, but we're not even looking at cyber criminals who may not even have the oversight and processes of a government. So to me, that's sort of what concerns me, what we're looking at at the threat landscape right now.

Brian Contos:

Yeah. I mean that brings to mind, you know, statements that sometimes you hear that you no longer need to be a nation state to wage war, right, especially cyber. You don't even have to have those types of resources that a intelligence agency or a group of the military might have. It could be a splinter cell, terrorist organization, organized crime group, you know, just general cyber criminal. It's interesting how much havoc can be raised.

Brian Contos:

You know, I heard these broad statements made a couple a couple of years ago, and I'm just wondering if you think this holds true, or it might be completely wrong, but I've heard that a lot of the attacks that we see coming out of Asia, while they're very high in volume, tend to be a little bit more commoditized, whereas the attacks that we're seeing out of Eastern Europe, in general, and these are all generalities, tend to be far more sophisticated, advanced attacks.

Brian Contos:

Is that kind of the thinking today or is that not really the case anymore? Is everything just sort of meld together at this point?

Sandra Joyce:

Well, you know, I think that it really depends, and you know, this is one of those questions that it seems very simple, but has a complicated answer. So if you think of NotPetya, right, it's just an incredibly disruptive incident certainly that came out from what we believe to be Russian actors. But looking at something like WannaCry, where we have attribution to, you know, North Korea, right?

Sandra Joyce:

So, I think that it really depends on specific threat actors and what they're willing to do. We've seen very aggressive behavior from Iran. We've seen it from Russia, we've seen it from North Korea.

Sandra Joyce:

I would agree that the activity that we see coming out of China has a different bend to it. It's mostly towards espionage. It's mostly in that realm. Some, you know, theft of intellectual property. So if we were going to put these into big buckets, then I think that, you know, we would probably struggle to say that it's one side or the other.

Brian Contos:

Sure.

Sandra Joyce:

Frankly, nation states are taking steps. They are taking reckless steps in many ways. And one of the things that, you know, our CEO, Kevin Mandia, has really spoken out publicly about is the need for us to have more cooperation across governments, have rules of engagement, some kind of agreements where these governments are going to agree that the implications for this reckless use of wormable malware that's going to propagate, you know, all over the world, that really nobody wins in that situation. So how can we come together and try to share information, regulate ourselves, you know, and look at what our militaries and our governments are doing and make sure that we are not causing unnecessary risk to the global community?

Brian Contos:

Yeah, that's fascinating. And I appreciate your point that this is all shades of gray. It's not as simple as one versus the other. So very well-stated. You know, if you could communicate one thing to our listeners about cybersecurity right now, what's kind of top of mind?

Sandra Joyce:

Don't click on it. Just stop clicking on it. No, I'm joking, but it just boggles my mind that like 90% of things are starting through email that people click on. But in all seriousness, I would say, you know, the adversaries are the ones that benefit when we don't talk about threat information. The adversaries are the ones that benefit when we get caught up in mistrust or red tape and all of the things that block open communication.

Sandra Joyce:

And so, I think that what I would say is the more open we can be, the more efficient we can be in the transfer of knowledge, I think is really the key. Because, you know, one company can't solve the problem. One government can't solve the problem. We need to come together in order to combat this. And the only people that benefit from, you know, keeping this to ourselves is the adversary.

Brian Contos:

Yeah. Yeah. No, I think that's a great statement. Well, Sandra, there's a question that I like to ask everybody on our show as we wrap up here, and that's who's your favorite superhero or super villain?

Sandra Joyce:

Well, I've been a big fan of Marvel, so I would say that Thor is probably my favorite superhero, but with a caveat that it's the Thor from Ragnarok forward, not the Thor before Ragnarok. He was a little too serious, but the Thor from Ragnarok forward is absolutely my favorite.

Brian Contos:

I'm with you. I'm with you. A superhero without a sense of humor? I mean, come on. Awesome. Well, Sandra, thank you so much, and thanks to our listeners for joining and be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.