U.S. Senator Maria Cantwell

Commerce Committee Hearing on Aviation Cybersecurity Threats

September 18, 2024

Sen. Cantwell Opening Statement

[AUDIO] [VIDEO]

Sen. Cantwell: Good morning. The Senate Committee on Commerce, Science and Transportation Committee will come to order. This morning, we are having a hearing on aviation cybersecurity threats. I appreciate the witnesses being here today.

The reality is stark: our aviation industry is under constant threat from cyberattacks, up 74 percent since 2020.

With the aviation sector contributing more than 5 percent of our GDP, $1.9 trillion in total economic activity, and supporting 11 million jobs, we have to wake up and take these aviation cyberthreats seriously.

As we saw in the 1990s, when weaknesses in the power grid exposed the system to catastrophic failures, we have a similar situation today in the aviation sector. Like with the utility industry, the solution has to be a strong national standard for resiliency, and organizations committed to the highest standard – whether that's voluntary as an organization, or something stronger.

Because every time we witness these technology failures, consumers are the ones left holding the bag.

Let me share a recent example that hits close to home. Last month, Seattle-Tacoma International Airport was hit by a ransomware attack from the Rhysida Group, forcing airport leaders to shut down various computer systems that run everything from ticketing to display boards to baggage claim, creating a confusing environment for passengers and workers, and yes, delaying flights and some flight cancellations.

The display boards were down for a week. I personally ran through the airport trying to catch a flight, not sure if I was going to the right gate. I had something on my device, but since all the boards were dark, I had no idea if I was going to get to my gate, or if that was really going to be the gate.

The displays were down for a week and employees had paper signs directing passengers on where to go to get to a gate. Check-in kiosks were down too, forcing passengers to wait in line for paper tickets. Other passengers endured long waits at baggage claim as airport staff manually sorted the thousands of checked bags in the terminal.

The airport's internal email systems and website went down, and the attack group, which is believed to be a Russian organization, is now threatening to release personal data from airport employees unless the Airport pays $6 million worth of Bitcoin ransom.

While most systems are now back online, three weeks later the airport's website and some internal human resources functions remain down today.

I appreciate … SeaTac's Aviation Managing Director, Lance Lyttle, who is with us here to discuss the impacts of this event and the lessons learned.

SeaTac's situation isn't unique. Across the country, we've seen troubling examples of cyber vulnerabilities in our aviation sector. In 2020, a hacker accessed internal systems at San Francisco International Airport. In 2020, San Antonio Airport had its website spoofed. And let's not forget the 2015 incident where a hacker claimed he had access to a United Airlines flight's controls through the in-flight entertainment system.

That is why we are here today– to spotlight this issue and figure out what more needs to be done. And to let the traveling public know that Congress and the Federal Government are going to combat potential disruptions to their air travel and safety.

The FAA Reauthorization bill, which was signed into law, included a subtitle strengthening cybersecurity, including directing FAA to establish a process to track and evaluate aviation cyber threats, and designating a Cybersecurity Lead at the Agency. And just last year, TSA and FAA both issued cybersecurity requirements for airports, airlines and manufacturers.

I'm grateful to have Marty Reynolds, a cybersecurity expert from Airlines for America, who is here to tell us about emerging threats to aviation cybersecurity and how the industry and government can respond.

Cyberattacks and other recent technology outages in aviation– like the NOTAM failure, or the Southwest meltdown, or the CrowdStrike outage – have made it clear that brittle infrastructure won't cut it.

In the aftermath of the cyberattack at SeaTac, Port of Seattle Executive Director Steve Metruck said that business and government "need to invest in cybersecurity" and "need to be prepared should a cyber [attack] gain access to systems."

When airport and airline systems are compromised, it also puts passengers' personal data at risk. For instance, in 2020 hackers stole the credit card information of over 2,000 passengers. And cyberattacks on frequent flyer accounts are up 166% in just the past three months.

The SeaTac incident created hardships for travelers—like nonfunctioning flight status [boards] and, as I mentioned, delays getting luggage. And it's easy to imagine a scenario where cyberattacks coinciding with other events could cause more cancellations or delays.

Even in these difficult situations, airlines must abide by their passenger commitments and requirements.

Mr. Breyault is here from the National Consumers League to remind us of those resources passengers have when dealing with flight disruptions. This includes requirements for airlines to provide hassle-free refunds as mandated by the FAA Reauthorization.

Thank you again to our panelists for being here. I look forward to your testimony.

Sen. Cantwell First Question

[AUDIO] [VIDEO]

Sen. Cantwell: Thank you so much.

Thank you again to all of the witnesses for your testimony.

Mr. Lyttle, you said something in your testimony that just needs a little more emphasis. You're saying our capacity at Sea-Tac is 30 plus million people and we are at 52 million a year, is that what you're saying?

Mr. Lyttle: Yes. We were originally designed, the current facility is designed for approximately 30 million, and we are doing 52 million this year.

Sen. Cantwell: So, we are already stretched?

Mr. Lyttle: Yes, we are.

Sen. Cantwell: In addition, you are doing construction right now, so that is an additional stretch?

Mr. Lyttle: That complicates it even more, yes.

Sen. Cantwell: Do you think Seattle was specifically targeted?

Mr. Lyttle: I'm not sure why we were targeted. Our understanding, we see that they have targeted organizations in the USA, outside of the USA, within the aviation industry, but also outside of the aviation industry as well.

Sen. Cantwell: So, you don't have any specifics on why you think Sea-Tac was, on this particular event, was singled out?

Mr. Lyttle: Not at this point.

Sen. Cantwell: What do you think - now, I know you are still in the middle of the investigation, and you also don't want to reveal information that may aid and abet others in this particular area, but isn't hygiene a particular aspect of this? We know this from other sectors that have been attacked. Isn't the ability for people to attack can come in in all sorts of very easy ways, from phishing and other events?

I didn't hear anyone talk about this as part of a concern, so just wanted to know where you are on that issue.

Mr. Lyttle: The various different cyber attacks, such as phishing or ransomware attack, denial of service, they are all concerns for us. We have successfully in the past thwarted denial of service attacks, phishing attacks, and we continuously do exercises. We have internal and external audits that we conduct on a regular basis to minimize the impact of any cyberattacks on our environment

Sen. Cantwell: So will we learn what exactly happened? Will we at least have access to that information?

Mr. Lyttle: We will be conducting an after-action report, independent after-action report, and that will be available.

Sen. Cantwell: Okay, and what is the timing on that?

Mr. Lyttle: We are not sure as yet. We are focusing on recovery right now, and once we have done that we will conduct the after action report, and we will share this industrywide as well as with the Committee.

Sen. Cantwell: Well I think to the brigadier general's point, this information sharing is critical. And since so many organizations within our government think they have a hand in cybersecurity, which they do, this information sharing gets lost.

And what we have seen, whether it is other sectors, we mentioned pipelines, casinos got attacked, I remember talking to somebody in the first casino, no one said anything. The second casino, then it leaked out, the third casino, they wish they would have known because then they would have taken steps.

So one of the reasons we wanted to have this today is because we definitely want people to have information about these attacks and what we need to do.

Brigadier General Reynolds, one of the things that we've done is this rulemaking authority through the FAA bill, and an ARC, an aviation rulemaking committee being set up. Does A4A plan to participate in that ARC, yes or no?

Brigadier Gen. Reynolds: Senator, thank you for the question, and yes, absolutely. We are excited that the ARC has been established and look forward to the charter being released, because we would like to participate.

Sen. Cantwell: What do you think that can do to establishing some sort of focus, here, on cybersecurity requirements that airports specifically need to look at?

Brigadier Gen. Reynolds: I think anytime there is an opportunity for industry and government to work together to come up with recommendations generally provides the best set of recommendations. The opportunity to work directly with the FAA through this ARC we know can lead to better outcomes and better recommendations. So we are excited. It is the first time we've had the opportunity to work in cybersecurity specifically, so we are looking forward to participation.

Sen. Cantwell: It is fortuitous we have this process established.

Brigadier Gen. Reynolds: Yes, ma'am. Thank you, again, for putting that into the reauthorization. We are looking forward to it.

Sen. Cantwell: Mr. Breyault, you mentioned a lot of things here, and when you think about it, the consumer is who we are trying to protect. We are trying to protect our citizens, but we're trying to also protect consumers from the impacts of an underinvestment in this particular area. What you think is most important in that, in the protection of the consumer? Is it at the airport and ticketing, or do you think that these are leading to individualized attacks as you said, as that information is then available on the web?

Mr. Breyault: Well, Senator, I would say that there are vulnerabilities that impact consumers throughout their interaction with the aviation industry. There are vulnerabilities that impact the safety of the data they provide, for example to rewards programs or frequent flyer miles, through the information they

share with TSA for security purposes, through the actual physical impact that they have when these events happen. Being stranded at the gate, missing important family events, running through the Sea-Tac airport not knowing which gate you are supposed to go to, are all impacts that happen.

And so, I think that the cost here really needs to be measured in, how do we help consumers recover when these occur? Because all of the investment, that I'm glad to see A4A and other industries making in this, is not going to prevent all of the cyber attacks. As General Reynolds said, there is no silver bullet, and I completely agree with him.

So I think what we also need to do in addition to thinking about how do we prevent these cyberattacks from happening in the first place, how do we create incentives to help consumers recover when they do occur? Because ultimately they are going to occur, and consumers are going to be impacted. So what do we have in place to help make sure that those harms are mitigated as much as possible?

Sen. Cantwell Second Question and Closing Remarks

[AUDIO] [VIDEO]

Sen. Cantwell: Thank you, Senator Markey, and thank you for your leadership in the FAA bill and getting those provisions to protect consumers. And yes, we're hearing more about the theft, particularly today of the mileage program and the need to protect that. But again, appreciate your leadership and communication on this.

I'm just going to ask a couple of just, round up questions, and I think we're done with other members here, and then we'll adjourn.

But one of the key messages from today is the need for communication, and I want to clarify, now, what is that immediate step on impacting that communication, best practices? We know that there is an ARC process at the FAA on cybersecurity. Much bigger picture. That's going to take a while, but what now are we doing. So, Mr. Little, who is the lead investigator on this attack? Is it the FBI or -

Mr. Lyttle: Yes, the FBI.

Sen. Cantwell: Okay. And then what would the witnesses suggest is the best communication framework right now, until the ARC process works, to communicate to other airports, the best practices and things that should be implemented from this? I would like to see a list.

One of the reasons we gave the NTSB an annual report requirement is because we didn't feel like people were emphasizing enough next steps after some of their indications from accident reports, what should happen. And so, they have now done that and I thought it was very successful, they came before the committee and basically said, yeah, these near misses aren't getting addressed, and then the next day the then acting administrator convened and put out a requirement.

So here we're trying to get the same level of response. What would you suggest, Mr. Breyault or General Reynolds, too. What in the near term is process?

Mr. Breyault: So, Senator, from a consumer point of view, clear communication and actionable communication from airlines to consumers is incredibly important. From the time the breach, or the cyber security incident, will first impact their travel, consumers need to be made aware of that.

Consumers often show up at an airport, in the CrowdStrike instance and we heard, we saw report after report that consumers were confused. They didn't know what was going on, they were getting mixed messages from the airlines and other sources about what the status was of their flight, and if they were gonna have to wait 30 minutes or the flight was going to get cancelled.

So I think it's really important that any cybersecurity response plan have a component in there about communicating with the passengers about how this will impact the flight that they're waiting for at the airport that day, or the flight they're going to leave home early in the morning to catch the next morning.

Sen. Cantwell: Mr. Reynolds, since this is a airport issue, but it affects airline capacity, what do you think the tool is for right now streamlining best practices and communicating that?

Brigadier Gen. Reynolds: Senator, it's a very important question. The industry relies heavily on standards, and in fact it's been founded on standards in many ways, and it's driven our safety record to the level that it has largely because of standards. I would start there.

It does take time to create the standards. It does take time to actually, you start with the best practice, then you start moving into the standards. I think the tabletop exercise we all talked about, I think that's also a very effective way for us to communicate with one another. We also participate with the Aviation Information Sharing and Analysis Center to share information back and forth with their members and our members as well. And I think the other part too, I just referenced, is it any opportunity for us to work closely with the federal government, either working groups or opportunities for us to share lessons learned, is beneficial for not just the industry, but also for the government as well.

Sen. Cantwell: Well, I think – does that exist right now? I'm saying I'm not sure that exists, that framework, right now.

Brigadier Gen. Reynolds: Now we are working with, on the information sharing, we are working with TSA, FAA and others to develop and work with them on this very topic, information sharing. The TSA, in fact, they have an intelligence and analysis cell that has been very helpful. They lead, in this case, we have meetings with them every day to talk about what's happening in the environment. There seems to be a really nice set of progress checks with them and the FAA and others to find ways in which we can improve information sharing. But it is. it's in the early stages.

Sen. Cantwell: Yeah, I just keep thinking about NARUC, and I was looking up trying to remember what its acronym stands for. But it's basically a voluntary utility organization that decades ago did the same practice. Why? Because they were being impacted so much.

And so I think that we have to figure out here how to formalize this now, while the ARC rulemaking process at FAA is going through, to see what we can get from a, just communication, daily communication. As was said, people want to know, well, what's the next best thing to implement. And I'm pretty sure here it's going to be related to hygiene, which is pretty simple and pretty basic, but

something that could get emphasized. And so maybe that is the FAA putting that notice out, or maybe it's also the industry working collaboratively, and so that's what I think, we need both, in my opinion, we need both. Because the industry can work very collaboratively, very quickly, and they know the systems they're trying to improve.

One thing, General Reynolds, since you're here, in our state there's been a lot of collaboration with the Guard and Reserve, because there's so many people who work in IT and are our State Guardsmen, and they would like to play a more active role here. So when you talk about the workforce shortage, you're thinking, well, what could they do to just hammer home this hygiene issue, and be part of a response? I don't know if you have any comments on that.

Brigadier Gen. Reynolds: Absolutely, ma'am. I have business cards I'll hand to you, and if you have anyone who's interested in joining the airlines, we would love to have them. Phenomenal capability, I'm very familiar with the folks up there in your state, phenomenal capability, because they have their day job, the insights they can bring to the military is phenomenal So appreciate you mentioning them, the Guard and Reserves do a phenomenal job in this space.

Sen. Cantwell: Well, I think they know – what's their job, to protect us on critical infrastructure. So we've had this discussion with them in Washington, in the State of Washington, on cybersecurity for many years. And I know I think I had Senator Murkowski come to an event on this many years ago when we were looking at vulnerabilities, particularly in schools, and they were active, and they had been deployed, there was a lot of cooperation between entities.

But as this need continues to grow, and it's not just going to be in the aviation sector, other sectors, where are we going to get that workforce, and how are we going to get these evangelists out there communicating to people.

But I thank everybody here, I think the key takeaway is, better protection for consumers on mileage rewards programs, better communication to airport infrastructure and airport employees to harden our resources. This is a growing issue, it's not going to shrink. The best way to do it is communicate what we need to do to harden those resources.

Is that right? Is that – Okay.

Well, I thank all the witnesses. The record will remain open for four weeks until October 16th. Any senators who'd like to submit questions, do so by that time. And then two weeks from now, we will have the record complete.

So thank you so much. I appreciate your willingness to respond to our colleagues. We're adjourned.