CyberAttack_mixdown

Wed, 1/13 10:37AM 56:41

SUMMARY KEYWORDS

attack, kevin, software, intrusion, norms, companies, cybersecurity, country, hack, microsoft, espionage, supply chain, cyber, katie, solar winds, vulnerability, question, world, people, organizations

SPEAKERS

Katie Moussouris, Tricia Johnson, John Carlin, Kevin Mandia, Senator Mark Warner

T Tricia Johnson 00:10

This is Aspen Ideas to go from the Aspen Institute. I'm Tricia Johnson. The nation's cybersecurity defenses are failing. Last spring Russia infiltrated computer systems of federal agencies and American corporations. Luda, security's Katie Massara specializes in defending organizations from Digital attacks in the wake of the armed insurrection in Washington DC last week. She says social media companies late response to foreign and domestic disinformation campaigns has dramatic and it's critical to shore up online defenses.

K Katie Moussouris 00:40

They will leverage whatever means necessary to drive further wedges through the existing divisions and inequity in our country. And there's clear evidence in other countries that this type of violence is fairly easy to incite and amplify, and be used by sophisticated and unsophisticated actors all together, that this kind of destabilization at a massive level and galvanizing of folks who have extremist views and the grooming of extremists and the cultivating of additional extremists, especially in domestic terror situations here in the United States. We've had tons of evidence of this

T Tricia Johnson 01:22

Aspen Ideas to go open to compelling conversations from the Aspen Institute. today's conversation is from Aspen digital. bad actors exploit digital vulnerabilities in governmental, corporate and individual networks. Kevin mandia, is CEO of fireeye, the cybersecurity company that uncovered last year's massive Russian hack, Senator Mark Warner as vice chair of the Select Committee on Intelligence. They joined Katie Massara in a January 7 conversation led by john Carlin of the Aspen Institute, cybersecurity and technology program. They discuss how the Russian hack was discovered and what it means for the future of digital security worldwide, including how to assign responsibility for cybersecurity and social media failures and define what is normal in digital espionage. Senator Warner also shares his assessment of the damage of the foreign led cyber attack compared to the domestic insurgents he experienced personally at the nation's capital. Here's Carlin.

John Carlin 02:16

I want to start with you, Kevin, how did you discover this was turned out to be unprecedented, perhaps in size, scope and sophistication? In terms of an attack by a foreign adversary? How did you discover it?

Kevin Mandia 02:31

JOHN, there's initial detection. And then there's, you know, doing the full forensic investigation and finding the backdoor. But I think you're alluding to how do we detect it in the first place? Is that correct?

Katie Moussouris 02:42

That's right. And I just want to echo on, maybe make clear that this is an instance where it's a it's a sophisticated foreign adversary, they hacked into that the potential to hack into 1000s and 1000s of companies, apparently, they have hacked into both commercial companies, and in the hundreds, along with government agencies, and they went undetected for many months. And then it wasn't, wasn't a government agency. It was you and your team who found them. And so first, thank you, because it uncovered a threat to our national security, but also how the app?

Kevin Mandia 03:20

Well, I think, first, we're not like every other company, what we do for a living is we have over 500 people that have 1000s of hours a year of investigating computer security breaches. So as we're doing this call, john, we're doing over 155 Security Investigations worldwide. So hacking in does I mean, what we do is we respond to that. But in this particular case, the event that got briefed to me that made us escalate and kind of declare this a full blown incident was that somebody was accessing our network just like we do. But they were doing it with a second registered device. So we called that person and said, Hey, are you did you just register a new phone? And he said, No. And I was actually even though it's a severity, zero alert, to some extent. For us. That's what I got classified at. We had somebody bypassing our two factor authentication by registering a new device and accessing our network just like our employees do. But it actually wasn't our employee doing it. And the minute we saw that we recognize that's the kind of tradecraft the most advanced groups would do the best hacks in the world. How about no malware? How about just use credentials and masquerade with all the noise by doing exactly what your employees do when they go to work every day? So we just detected it by seeing an anomalous login, and perut you know, basically saying, hey, john smith was at you logging in? No, it wasn't well, then it was a bad guy named john smith logging in. So the bottom line, that's how we detected it.

K

Katie Moussouris 04:57

And some people I think, assume that If you if you have the build a wall high enough or deep enough, you can keep a dedicated adversary out of an internet connected system. This along with many other cases, I think is a wake up call that even the best you can't keep them out. But you can try to do is, is detect them once they're in. But here they got in through a particular means called the so called supply chain or software supply chain issue, you can just walk through a little bit what what that means?

K

Kevin Mandia 05:29

Yeah, absolutely. You know, we just told you how we detected the breach, john, when we started doing our investigation, we had a network kind of pre wired for this sort of thing, you know, capture as many packets as possible at forensic software on your endpoints. When we started investigating this looking at 1000s of computers trying to figure out have they been accessed unlawfully or without, you know, by somebody without authorization, we kept backing into the earliest evidence of compromise for us kept coming up a system that harbored the solar winds product. And after exhausting virtually every other means of entry, we decided it's time, you know, you never want to start there and say, let's just reverse a platform that we bought from somebody. Because most companies use hundreds, if not 1000s of people's software, and to decompile it, reverse engineer it and find malware in it when the malware is obfuscated is not a simple task. So we just kind of honed in on a particular server happened to be solar winds, exhausted the friends at gleeds everywhere else and said, Okay, we've got enough to go on now. So we decompiled. You know, basically, there's about 14 gig gigabytes of files that make up the platform. There's over 18,000 files, I believe, we kind of looked at 4000, executable files, decompiled it into millions of lines of code, and then found 4000 lines of code that were malicious. But it's not where you'd start. And that's the key to this. There's no magical wand that finds backdoors in software that we all purchase and trust. And what led us to really do all that work, john was in fact all the forensics, the 1000s of hours of forensics we did prior to recognize that solar winds needed to be reversed.

K

Katie Moussouris 07:20

Thanks, Kevin. And as we hear that they this threat actor happened to target the world's best investigative response firm who was able to find essentially through a stack the needle going through 1000s of lines of code to find what had been hidden, and what's an otherwise effective and useful product. Katie, you've been sounding the alarm bell about that. For years. What should we learn from this supply software supply chain? attack? And from your perspective, how does this differ from other major cybersecurity incidents? Well, you know, what Kevin was alluding to, in terms of the means by which this actor got access to their systems is, you know, exactly right, in terms of what an attacker would want to do, as in masquerade as legitimate users. And they happen to do that through a software supply chain attack, where, you know, they compromise solar winds primarily. And were able to forge you know, forged signed updates by solar winds, so that, you know, this trusted vendor that is in, you know, at least 33,000 different organizations with the software in 18,000 downloaded the backdoor version, you know, that was where the software supply chain attack occurred. But the same type of access on a less savvy target than fireeye would have been fishing to achieve the same, you know, type of result of getting in through and then masquerading as a trusted user to gain further access, you know, post exploitation type of activities to winnow your race further through a network is really, you know, the the parts of this type of attack that we've certainly all seen before, I think the unusual bits, you know, that, that we have seen, you know, some evidence of this happening in the past, see, CCleaner was one of the ones that was used in wormable attack. And that also that software was also, you know, backdoored in a similar way to solar winds, where the attackers first attack that software replaced the binaries with some malicious ones. And then those trusted binaries were then, you know, installed as updates by the customers have Si, si clear. So we've seen this type of technique used to affect the supply chain. And one thing that I think that people have been missing in terms of the overall plot of how unusual is this is that the original software supply chain attack was your operating system, right way back in the days of, you know, the early 2000s, late 90s, early 2000s. You know, really the software that lived on top of your OS operating system certainly was going to be vulnerable to two security holes as is every piece of software. But your trusted supplier, your trusted vendor that was you know, that could potentially affect every computer worldwide. At the time, it was over 90% Microsoft. Right. So Microsoft itself was the original supply chain attack vector for most for most organizations. And that's something that, you know, we try to sort of make this into a different thing and recategorize it as all new, but every single component of this attack is not new. I think that was your question. Maybe you had a follow up that I haven't quite answered yet. Well, then I'll just follow up a little bit on this, because there's been discussion and Microsoft has publicly said, both that, as you say, elements of their system were used to effectuate the hack, but also that they were hacked, and that some of their code may have been at least viewed What are we to make of that, in so many systems are reliant on Microsoft? What what are people to do with that information? Well, you know, I think for for consumers, and the enterprise, the same thing that they always do, which is, you know, trust that Microsoft is doing an investigation, much like fire I had to do to ensure that its systems are as clean as they could be. The fact of the matter is, you know, what, access to Microsoft source code really gets an attacker is potentially, you know, some ways to find new vulnerabilities in order to exploit them. But a much more direct method, if they had access to Microsoft's network is to go straight for the bug databases themselves, and mine them for every single unpatched vulnerability that exists. You know, Microsoft hasn't come forward and admitted any kind of access to its vulnerability databases internally. But that would be much more concerning to me. And quite frankly, if this attacker is as savvy as we all think they are, let me just pause you for a sec, to make sure people are understanding what you're saying. So you're saying that Microsoft keeps a database that would show where there are bugs or vulnerabilities in their systems that could be exploited. All software houses have to keep vulnerability databases, if they are to track vulnerabilities in their code that they are working on. It's the same as any other bug database. And often they are the same database. So your general bugs, and your security bugs, they all live in the same house. In a lot of cases, Microsoft does have, you know, some living in the same house as the product security teams, bug databases. But this is a natural component for every single software house that cares about tracking its bugs, whether they're security bugs are not security bugs, they have to have a database to track all of these things and the work in progress. So that's a normal part of business operations for software, software companies. And in turn to Senator Warner, but just start by thanking you, Senator Warner for for joining us. today. I think we all watched with distress and heart the events of yesterday and your presence here your actions last night are a demonstration to the world that is that is watching that, that violent thugs will not keep our democracy from working for foreign nation adversaries that remain on guard unable to to handle the threats that they pose, specifically. So thank you for for being here. And specifically Russia. I want to talk about with you in relation to these, these events, the intelligence community, it said that this was probably of Russian origin. What, what steps or actions are you contemplating? Do you think Congress should be contemplating to try to reduce the risk number one, as we look forward to next year, and number two, to ensure that there are consequences for those that intrude upon our systems?

S Senator Mark Warner 13:57

Let me thank you for having me. And I want to I do want to answer your question in a moment. I also want to acknowledge what you and Vivian already indicated. Although it has been very rare that I've ever seen Kevin with a tie on.

14:13

But

S Senator Mark Warner 14:15

you Microsoft to a lesser degree, but fireeye. In particular, what Kevin firm is firm did was as candidly as kind of patriotic and action, as I've seen from any enterprise for a long, long time. I think it has been clear that we might still not know and this will go when I answer your question about kind of necessity of of reporting and what type of reporting in fact that Kevin not only notified but then laid out in full detail how the attacker did attack and the methodology used the assets. They they got access to, didn't have to do that. And we USG writ large, but I think private sector as well owe him and his firm a debt of gratitude. But I want to I just, I cannot, with this group here and with what's happened in the last 24 hours, not speak to it for a moment, because we're talking about here a nation state attacking or intruding. Again, even terminology we have to be careful with. And I'll come back to that in a moment. But intruding into government networks and private sector networks. And we have to be concerned about, you know, what information they gained, in kind of this great power competition, but whatever, Russia, and we know who it was. And this White House again, has watered down the attribution statements that should have been made in one more outrageous effort to constantly underestimate and under report on Russian activity, whether it's election activity or otherwise. But for all the damage that was done in this intrusion, it pales in comparison to the damage done to our country in the last 24 hours. One of the things I'm proudest of in this job has been the Senate Intelligence Committees report on foreign interference. Work with Kevin on that he was a great help educate me and a lot of my colleagues, one of our top recommendations out of that report was that any candidate or elected official ought to tread very gently and carefully when you go out and question the integrity of our elections, because at the end of the day, what we have always presented ourselves is that our democracy is different that we abide by rule of law, that we adhere to a set of standards that we had peaceful transfer of power that is more powerful for our country than all the planes and ships and bombs that we have. And in Donald Trump, we have someone who's abused that to an unprecedented level before the election even took place, he was threatening to undermine it if he didn't win. He has lied repeatedly for the last two months. The point 35 to 40% of the American public, don't believe the election returns don't believe the recounts don't believe our judicial system. And has led him and his enablers which we then saw the logical conclusion of that kind of big lies and disinformation campaign accelerated by countries like Russia, through technology take place and play out yesterday when literally 1000s of thugs took over the Capitol and desecrated the Senate House. Four people were dead 60 law enforcement officers are wounded. And the amount of damage the physical damage to the building can be repaired. Last night, thank God, you know, 90 plus senators of both parties stood up for the constitution when I was not nearly as eloquent but I when I stood up, I wrote the rules and showed a picture of what was on the front page of one of the German newspapers, these thugs in the halls of Congress. The images that have been conveyed around the world in the last 18 hours in every forum for us, is a bigger goldmine and more priceless the Vladimir kooten than anything that Russia has obtained out of this intrusion. And until and unless all of us I don't care who you support it for precedent, are willing to stand up for rule of law and willing to call out lies and disinformation and misinformation. Then we're over here fighting this intrusion, which is serious. But when the whole basis of what is the strength of our system is at risk. And the collaborators are not simply those self serving politicians who are actually raising money yesterday off of these crowds or giving fist salutes to these thugs. But the collaborators include some of the wealthiest companies in our country. The Facebook's the Twitter's the Googles who allow this kind of disinformation misinformation from Form sources and outright lies, to perpetrate their platforms in a way that 35 to 40% of American public believes that the election was stolen or manipulated, or that our whole court system was wrong. And their 11th hour conversion now to suddenly take down Twitter's Facebook feed or,

20:23

or,

S

Senator Mark Warner 20:24

or take down Trump's facebook or twitter feed for the last two weeks is way too little too late. If they had one ounce of the level of patriotism that Kevin Mandy and fireeyes had, we wouldn't be in this position. And I'm obviously pretty damn angry. My anger is not from the Senate Intelligence Committee chairmanship ship or the Democratic Senate. My anger is an American elected official who believes in this country and believes in our system, and it is under full frontal assault. So I'm happy to take on this question, I will answer it now. But for anybody on this line that thinks that the most important action is this Russian hack, when we saw the images, luckily, we we certify the election last night, and the vast majority, at least in the Senate, 90% plus did the right thing. But the price will pay for those images, about anything special about our democracy or the fact that says the Syrian government today attack, the hypocrisy of America calling itself a democracy is going to be a much bigger price. Then the information that's being vacuumed up by Russia, in this in this intrusion. And the fact that again, as recently a couple days ago, the White House watered down the attribution. Responsibility is again, extraordinarily disturbing pattern of this White House's continual failure to call out and its agents time and time again. Now, where do we go? From from here? You know, one of the questions that we are continuing to ask my boss, Kevin, and he's brief, my committee, the past, the Microsoft folks will try and ask us, gee, we had yesterday, FBI, NSA, and sissa. As well as representative odni. In before the committee, we have a huge amount of education. You know, I've got colleagues who are out there making comparing this intrusion to Russian jets flying over the Midwest of our country. It's not that it's not a not Pecha denial of service complete taking down our system. But I do think we have to decide is this within the bounds of acceptable espionage, countries spy on each other, but the volume and level, both in terms of governmental entities, and in terms of private sector enterprises, and the level of sophistication is Kevin and Katie have already pointed out, ought to be alarming to all of us. The fact that, again, this administration got rid of their cybersecurity folks at the White House in their first weeks. One more indication of where at least they place this priority, we're gonna have a chance to turn the page in 14 days. But we need to at least start with how we define this where this falls on this continuum. If you've got traditional espionage here, and not Pecha denial of service, and takedowns. Here, where is this along that we need to make clear, this is something and Kevin since we visited, we need to make much clear how many other foreign nations have been attacked, and they need to come forward so that we can create some level of international norm setting and some rules of the road because I think Kevin has pointed out when, when I first your adversary brings, it's a game against any enterprise, public or private, particularly on the non classified side, chances are, they're going to be successful. So better cyber hygiene alone is not going to win the battle, we're gonna need some international norm setting. And we're gonna need, I think, a full review of the obligations of reporting from public, the fact that the public enterprises don't even have to fully report the system, let alone the fact that the private sector, if a company doesn't reach materiality has no obligation to report I think needs to be fully fully reviewed. So we have to educate our colleagues, we got to set some norms, and we have to look at the policies so we don't have to rely upon the goodwill and patriotism of someone like Kevin mandia to make sure our government was was notified. Just think, you know, when we see the abuse taking place, and the Lies and disinformation that are perpetrated on on some of our social media platforms. If we had to wait for the same kind of patriotic leadership from Facebook, Google and Twitter, we'd end up with thugs attacking the cat. But well, that's what frickin happens. And before we kind of realize that yesterday, changed our country, probably more than what the Russia attack is going to change, we got to look at both of these sides in terms of our all of our obligations, I think public sector and private sector devote truth, the rule of law to ferreting out the bad guys calling them by name, and then having a counter strategy. And I apologize for going on a little bit, but it's been one hell of a last 24 hours. And that, again, we're gonna get better, we will do better our country will get through this. But the images that are across the world of these clubs, and our capital is going to do more damage to our country than anything which is done in this intrusion.

K

Katie Moussouris 26:06

Thank you, Senator, again, both for being here. And showing that regardless of the actions that they take, that you and your colleagues will not be cowed, and that democracy will continue. I want a lot of important threads and in what you said, To follow up on a little bit with the panelists. So one, there's the problem of allowing inaccurate information, false information to flourish incitement to occur on social media platforms. And we've seen that problem, as one that's been amplified, sometimes originated by foreign actors. In the case of Russia, and the dissenters pointing out that sometimes it's not, there's no foreign, there may not be a foreign actor, or the foreign actor may not even be amplifying it, but it is still a threat to our democracy. If it's not appropriately monitored. I know that Kevin, that's not your area, I might turn to Katie to see if you have thoughts on that. And then secondly, because I'll open this up to a little group. That senator also touched on the fact that as we look at the range of activity that foreign actors can take against the United States, through cyberspace. You have that threat amplification of false information, you have intrusions into systems. And intrusions can be used to cause damage, like not Pecha, they can be used to steal information with economic value, as we've seen case of China, among others. But in this instance, it looks like the motive behind the attack was the collection of intelligence to was done on scale. And it was done through through supply chain. But does that make a difference? Or is this more routine intelligence collection? Okay, maybe I'll start with with you. curious, what do you think of the responsibility of social media platforms to police content, especially particularly content that might be used to incite violence or other activities? And how do you distinguish that between intrusion or nation state amplification activity? Well, you know, social media is not actually my area, either. You know, but what I would say is, you know, the disinformation campaigns that we've seen, you know, they will leverage whatever means necessary to drive, you know, drive further wedges, through the existing divisions and inequity in our country. And what I think is been dramatic about the lateness of the response from social media companies has been, there's clear evidence in other countries, that this type of violence is fairly easy to incite and amplify, and be used by, you know, by sophisticated and unsophisticated actors, all all together. So they had ample evidence already, that this kind of destabilization at a massive level, you know, and galvanizing of folks who have extremist views and the grooming of extremists and the cultivating of additional extremists, especially in domestic terror situations here in the United States, we've had tons of evidence of this. So you know, I would say that this is definitely something that, I hope, I hope that the next Congress takes on as, you know, what exactly is their responsibility? But yeah, that's, you know, not really my area when what Senator Warner said that, that I noticed and picked up on is the idea of setting norms in cyberspace is one that is thrown around a whole lot. And where I keep having this feeling is much like yesterday was, I think, a huge surprise to everyone what happened on Capitol Hill, even though we all knew there was a potential for an explosive type of reaction. I don't think anyone could have predicted that. That kind of desecration of our democracy that happened yesterday. Similarly, in the norms category in cybersecurity, I have this, I have this growing feeling. And I have for several years since norms conversations have been, you know, in in my purview, and as I helped, you know, renegotiate the wassenaar arrangement for cyber export controls of cyber weapons, on behalf of the United States as part of that official delegation, the idea of setting norms, it feels to me, like we're in the decline of the digital Roman Empire, and we're trying to tell people that it's not okay to use elephants to cross the Alps. Meanwhile, they're using elephants to cross the Alps, and we will be overrun. And I think that the time for us to be considering what kind of norms we want to exemplify in the world with our own behavior, our own cyber espionage that we absolutely must be able to do, right, this is something that you know, every country with the capabilities is, is going to preserve their, their right, and their ability to gather intelligence, you know, elsewhere in the world, balancing what our example setting should be in terms of those behaviors and those acts, but also understanding that in the world of cyber, and when it comes to things that we you know, we will lose hand, call them cyber weapons, this is not something that we can, that we can narrowly define such that we can appropriately regulate those things. It's regulation of the behaviors and what you do with it, as opposed to the technology that I want to make sure in these norms conversations that go forward, Senator in the next administration, the next Congress, but these norms conversations have that nuance that it's not the technology that needs to be, you know, under these norms, it is the behavior that we all enact, as, as you know, a global community that hope to preserve order in the world in general. Let me jump in on that, just as Kevin, know, what do we know about the motive of this operation? Are we assuming too much when we say that the motive was intelligence collection based on your experience, over the over the years are the things you can tell about the tradecraft or otherwise, that indicate what the what the motive would be? And what they actually accomplished?

K Kevin Mandia 32:18

I'm gonna do it every bad panel is does and answer the last question and then answer that question. You know, one of the things about norms and listening to Katy, I recognize just studying this for decades, hard to have norms for espionage, we can damn well have norms for ransomware, the whole world is sick of tolerating hospitals, pharma companies being ransomware. And watching billions of dollars leave the United States and other Western nations for the most part. And one of the best ways to crimp down and some of the bad actors that follow different norms. And espionage is in fact, to take a hard stand and have strong policy and international cooperation to shut down ransomware. So I think there are steps you can take. But in regards to espionage, thinking about it, there's too much asymmetry. There are too many nations that can't compete with us tanks or dollars, but can win in cyber because we're in the glass house in cyberspace. So I'd recommend the Espionage one hard to follow and find international norms for that, of course, we can set an example and people will follow it. But in regards to criminal rules of engagement across the entire interwebs, that's very doable. And we got to stop tolerating what's happened over the last 12 months 2020, without a doubt, the worst year for every chief information security officer in my 27 years of doing this, and it was driven by ransomware. So a policy on ransomware will in fact, actually be invoking punishment against the very people that probably did the breach that we're discussing here today. In regards to what they are after, at least I can speak on behalf of fire I'm this was an attack that stage one was getting a backdoor in your network in the solar winds platform. Stage two was actually using that backdoor, where the first step was to get to domain credentials, a secret server, some kind of server that has user accounts and passphrases so that they can access your networks or the victim networks the same way the victim employees do. Stage three was primarily to get the token signing certs to access an O 365. environment, probably mostly for email, and specific people's emails in stage four that call other and it'd be dependent on the victim companies at fireeye. They stole our red team tools. Those are tools we use to do proactive security assessments to see if attacks that we've responded to. And we've repurposed the malware for the most part. Do those attacks work on our customers networks? So for me, what I learned from this attack is,

34:57

you know,

K Kevin Mandia 34:58

throughout my history, I haven't seen a whole A lot of dot coms compromised for this kind of espionage. I've seen it from China against the defense industrial base, and hedge funds and everybody. But this group smells a little bit different has consistencies with a different country. and.com always felt almost off limits in my 20 something years till this breach. But you know, I'm not an expert on what's fair game and what's not fair game for espionage. But we lost our red team tools.

Katie Moussouris 35:27

I want to just speak up there about the precedents in the past of nation states attacking, you know, private industry, you know, we had the Sony attacks, right which nation state, we also have the Aurora tax. And that was a decade or at least over a decade ago at this point, where that was China. And they went for Google, this was another, you know, they went for Google, they got Microsoft, Apple, a bunch of these different tech companies. But what was interesting, that was another software supply chain attack, Google had been running outdated versions, I think, probably for some app compat testing internally outdated versions of Internet Explorer, inside of Google. And that is how China got in to Google was with some older versions of IE. So we have seen this pattern used, you know, over it for over a decade in terms of attacking private companies doing it on mass, I think, you know, what I've noticed in the last 20 years of my career in cybersecurity, is that we have these arcs of coverage, right and so much of policy, and is shaped by news coverage, so much of news coverage is, you know, shaped, certainly by sources like us, you know, but, but over the years, the amnesia that sets in that this is something that we've seen before, or these components we've seen before, I think that clouds policy in a big way. And that's something that, you know, hopefully with experts like Kevin, and you know, hopefully they, you know, other folks that the new administration will bring in that have real world expertise at this grand global scale. because there aren't that many companies that spanned the globe, I mean, certainly tons of them are in the United States, right technology companies that are part of the supply chain in the United States. But that also goes back to the fact that 2008 was when I created Microsoft vulnerability research, which sole purpose was to coordinate vulnerabilities that affected multiple parties, not just Microsoft back in 2008, because there was already a need for that level of coordination across private companies. So anyway, I'm I'm, I'm hopeful that because we lost time, with the disorganization of the previous administration, and its lack of focus, and being in denial for various purposes, of what we're up against cybersecurity wise as as a nation, I think it's really it's high time. And I have, I have a lot of hope that we can start getting it right. Again,

Senator Mark Warner 37:59

I agree with what Katie said, it's hard to attack the technology and not to be the usage. But there you have it again, and you guys had a lot more expertise, and I there seems to be at least areas that ought to have some level of discussion here, it took us three years to pass a bill to have basic IoT cybersecurity standards, that's lunacy. You know, when the government spending billions of dollars buying devices that were unpatentable that had embedded source in an access codes into them, the fact that we have mentioned that there are plenty of like platform companies that have known invalid software out and there are no repercussions, you know, on that, does there need to be a debate about a liability, we, you know, does there need to be a higher standard amongst companies who are doing patches, as opposed to just basic security. Kevin, I think, you know, the, my understanding at least is the level of sophistication, this intrusion was such that while they they got in the back door, they then went through the window, they were then inside is the way you describe the fat, thank God, they only went at selected information because they wanted to narrow the universe to make sure they weren't detected. Right. But the ability if they'd had other motives, in terms of moving towards denial of service on a broad based approach here, yo, it could have been much much more so and I get this the norm stuff is kind of squishy, but if but what what I would hope we would get to and we you know, and, and my knowledge level amongst policymakers is high, but it's peanuts compared to you guys. So you got to help educate us. Is that and why do you think there's still some golden In international, if this is simply, if the rest of the world views this is, alright, Russia is hitting the United States, United States and Russia, and this is the back and forth just on their espionage battles. And they can turn a blind eye to it. But if this is suddenly a supply chain across a multiple of public and private enterprises in Germany and the UK, Vietnam in a number of other places, and in and it's in, it's a level of intrusion, that could lead to denial of service, maybe the attribution standards ought to be lower, and there ought to be, again, a uniform response that we're going to punch you back in a much harder way. And it also still begs a huge question, because the number of brand brand name players that are involved in this, what we call solar winds intrusion right now that have not come forward. would surprise the hell out of many of the people watching this? And can we ever respond if there's not some requirements, that that there's some requirement of reporting here are some requirements notification, and, and the idea of where we notify in our government right now, I get the fact that notifying the FBI whose goal is not to stop attacks, but to actually investigate criminal procedure may not be the right thing. Maybe there is some third party intermediate, maybe it is firing, and Katie's firm, that you turned him first, maybe it's an industry standard, but there's gotta be, there's gotta be some notification process. That's absent now. And we're not going to get it 100%. Right. But what we're getting now is pretty much all wrong. And, and again, even our top folks in in USG have acknowledged that without fire eyes, Revelation, this intrusion that's been going on long over the years, we all know could still be going. That's not a good way to protect ourselves. That's like, you know, counting on Facebook, Google and Twitter to do the right things when you've got a disinformation source not only coming from the Gru, but coming from 1600. Pennsylvania Avenue, K

Katie Moussouris 42:18

you referenced the idea that currently, there's insufficient reporting, and then perhaps we're not paying much attention on the reporting to how to defend our systems or learn from it. A member of the Aspen cybersecurity group Alex Stamos, has called for the creation. And this has really been something around for decades, but for a version of the National Transportation Safety Board for cybersecurity incidents so that there's a place to report it and that the goal of the board is to learn from what's occurred in the incident. Right now we have a patchwork of reporting requirements that primarily fall around the set of personally identifiable information. But in this type of hack, that's often not an issue doesn't trigger the reporting. And that reporting is, is usually to consumers and regulators, and maybe use it to take affirmative action against the company, but it's not used to go into a repository for study. I think Alex's memorably put it for the hack that he lived through at Yahoo, that they did an incredible job finding out everything that occurred in that hack, but it all went to plaintiff's attorney. And it's sitting there still closed and litigation so that no one could have access to it. What opened us up to the full panel, what were the folks think about that idea of having a national board that could review these incidents?

S

Senator Mark Warner 43:46

I think it's an interesting idea. I think there may even be similar analogies in the financial sector where there is no shortage of the SEC. There is saffman, other kind of industry related entities that are first line of defense to report to, I think it ought to be ought to be explored, simply going to the FBI, or even simply going to sissa. And I think that Chris Krebs in particular has done a great job there. You're running our elections. Security isn't isn't solving the problem that yes, I've been. I've had bipartisan national Breach Notification legislation for six years, it's still crazy that we've got this quilt work of requirements, but if we're going to rely upon as you said, You're either getting into the trial bar or a company reaching materiality, or only PII as mandatorily reported, and then we simply have to, you know, rely on the goodwill of CEOs, you know, to do the right thing. Thank God we had Kevin but as we know, Facebook didn't do the right thing in 2016 when the Russians were all over their network.

K

Katie Moussouris 44:54

Well, I was gonna say that, you know, it's an interesting idea, but it's also one you know, The reason why organizations don't volunteer this information to the government or to even to, you know, coordinating bodies amongst themselves at a certain size organizations, you know, prefer to keep this in house because often, you know, more times than not, they are suffering from some level of cybersecurity hygiene negligence in some area, they missed something Something was left unsecured that should have been, and I think they're probably worried about the liability implications. So I think that, you know, if it were to be explored, and Congress has the power to, you know, include some sort of forgiveness for negligence, in some instances that would be found as a result of these, you know, sort of group forensic activities, then that's potentially viable. But without that, I see no way that any organization would want to expose its, you know, its internal flaws, its process failures and its mistakes to a broad group. That being said, you know, there's a there's a wide berth of what's considered to be diligence versus negligence in what we've seen inside of organizations. And you know, my, my biggest example, in my area of expertise is what I call bug bounty Botox. When organizations say, we care about security, and we've got a bug bounty and look at all the money we're paying and bug bounty. Well, you look under the hood, and you just look at the bugs that they're getting from their bug bounty, and it's low hanging fruit. Why didn't they catch themselves? Why are they congratulating themselves and everybody else is congratulating them on this, you know, this sort of performative security. So I'd worry about, you know, organizations, feeling like they had to hide every single, you know, bit of where their processes and their patches fell down internally, and not having a really, you know, really good way to gauge who's diligent versus negligent on on a, you know, on a more holistic basis, as opposed to that one incident and that one thing that caused that particular intrusion or problem

S Senator Mark Warner 47:10

Well, Kevin, Kevin, what Kevin answered, but I mean, I gotta just tell you, Katie, I, you know, if if we can allow the Equifax hatch hack to be basically built in, it's just the cost of doing business, and there being no consequences, which in effect is what happened, they took a hit for a while, CEO lost his job, but 146 million Americans, personal information was compromised by a foreign government. That's not a good long term solution respectfully, and it puts too much burden on Equifax or private enterprise. So be it.

K Katie Moussouris 47:44

Go? Absolutely. And I'm interested to hear what what Kevin has to think about this as well.

K Kevin Mandia 47:48

Yeah, I think, you know, in regards to this topic, there is a need for federal disclosure law, ultimately having a safe harbor in that law. So that, you know, the operating principle for it is you make other American organizations more secure, that would work, the unfortunate burden that will come with that is the assessment of whether that company was negligent or not. And, and to me, it's hard to prove negligence when you have a foreign power that attacks you. And so it's a tough one for me, though, I like the idea. The NTSB for cyber that does make sense. And maybe depends on who attacks you that kind of elevates or decreases your liabilities. Not all attacks are created equal. A lot of companies and and regulated industries are expected to withstand greater attacks than certain industries. So there is no one standard. If you make cupcakes for a living, you're not expected to be Fort Knox. So it's, it's a lot to sort out. But I think you could start with if there's an attack against an organization, if they disclose certain things in a certain way that helps the rest of nation defend itself and the rest of the organizations across the world to defend themselves. That should come with some sort of safe harbor, or you're not going to get to Katie's point, a whole lot of folks doing disclosure.

K Katie Moussouris 49:14

When it comes specifically to software in supply chain risk, there's been a focus on where it's made, and who produces it. And when it comes to the government contracting that's resulted in new rules about certain depending on the sensitivity of the of the software, sometimes it's only US citizens. There was reporting in the New York Times about a another variation, essentially this attack emanating out of the Czech Republic but with Russian coders. There's been discussion on the Hill about how to to address that. And again, I'll open this up to to the full panel but should there be rules or restrictions about where supply chain where your supply chain is hosted? To the who works on it. And even if it's not a rule or regulation, particularly Kevin and Katie, what would you guys recommend to your, to your customers or to companies that they should do to try to secure their supply chain? Well, the question is, should there be should there be rules about where your software comes from? I again, point to evidence where Russian spies were uncovered working for Microsoft as full time employees,

T Tricia Johnson 50:25

do

K Katie Moussouris 50:26

you remember this? This was another about a decade ago. So I don't think excluding, you know, foreign outsourcing companies is really going to solve our problem unless you move in a very dark direction, in my opinion, of requiring American companies to hire only certain ethnicity, ethnicities, and only certain citizens to to work for them. So I think that that one we I think, in my opinion, is is going going down the wrong path in terms of helping us secure ourselves in terms of securing yours, your supply chain one know what's in it, to understand that even as consumers, we're part of a software supply chain, how many of us have postponed applying our patches, right, when we're getting nagged to download the latest operating system on our phones? So you know, from the consumer to the enterprise to, you know, my customers, which are, include governments, absolutely, knowing what you have, knowing what their baseline level of responsiveness is to not just intrusions and incidents, but also non emergency vulnerability reports is often a bellwether for, you know, understanding how prepared is your supply chain to work with you end to end to secure some software? And I'd love to hear what Kevin and Senator Warner think,

K

Kevin Mandia 51:43

Senator,

S

Senator Mark Warner 51:44

let me jump in. I just think this. I would analogize. JOHN, your question to debate this. I'm also engaged in around 5g and Huawei you know, and and i agree with Katie, you don't want to wall off to certain ethnicities or only America, only those are not, you know, that is the kind of America only approach that we've seen recently, which is not a long term success. I do think whether we're talking we're talking here on on cyber slash software, as an old telecom guy, I think you can do some of the same conversations around 5g and next generation telecom system development, I think, you know, what we are seeing play out software, Telecom, Ai, quantum, we see, again, to Kevin's point, the asymmetric ability of a, of a country that can't compete with us militarily, but can compete in this asymmetric sector. I think we're also seeing, particularly visa v. China, a country that wants to set the rules, protocols, standards, in all of these developing technologies there China standards 2035 document ought to intimidate the heck out of all of us that it's you could imagine being written in the Kennedy era in terms of America's goals going forward. And they've got the resources and assets behind that. And in capabilities. I do think in this, I think there is this notional idea of a coalition of the willing, that would include countries that may have a commonality around cyber standards that may have a commonality around technology development, that may have a commonality in terms of belief in rule of law, that has belief in, for example, transparency, free human rights, that, you know, and, again, on some technical notice here, but those standards are reflected in 5g standards, those standards will be reflected in how you use facial recognition, those standards will be reflected in AI are in as we move into the whole question around quantum. And I think there will be an opportunity here. These are hard, hard things, to think about these tech technology related alliances in a 21st century way, the way we thought about military alliances in the 19th century, and then economic alliances in the 20th century. And that group of alliances ought to not just be five eyes or NATO, but are not a beat, you know, and somebody else would sign up would be the Japan and South Korea and Taiwan. And Singapore's and maybe the India's and Israel. I think that the UK Skype is something 12 idea out there. I think these ideas need to be explored. And whatever input I have into the next administration, I'm going to make that a priority. And I apologize for that. I'm going to have to sign off. I Kevin given the given the definitive answer on this, but let me just just I'm sorry, I've taken so much time on on the answering the first question, but I feel if you walked around the floor that the Capitol and you see the destruction that took place in the last 24 hours, and you see the images around the world of what our democracy looks like We all got to step up.

55:02

The bad guys.

S

Senator Mark Warner 55:04

I will stand by my initial statement gained a lot more long term out of what happened in the last 24 hours than they're going to gain out of this solar winds intrusion. And until and unless we're all willing, regardless of our partisan affiliation to speak up for truth at work Creek.

T

Tricia Johnson 55:24

Senator Mark Warner is vice chair of the Select Committee on Intelligence. Before entering public office, he co founded the company that became Nextel and invested in hundreds of startup technology companies. Kevin mandia, is CEO of fireeye, the global cybersecurity company that exposed last year's massive fraud and cyber attack. He's an expert in computer forensics with a long history in private and military technology. Katie mesorah is the founder and CEO of Luda security which specializes in defending against digital attacks. She's a self described hacker first hacking computers now hacking policy and regulations. She helped start the US government's first bug bounty program called hack the Pentagon. JOHN Carlin chairs the Aspen Institute cyber and technology program, and served as Assistant Attorney General for national security, helping protect the country against international and domestic terrorism, espionage, cyber and other national security threats. Make sure to subscribe to Aspen Ideas to go wherever you listen to podcasts. Follow us on social media at Aspen Ideas. org. Today's show was produced by Shannon Lewis. It was programmed by the Aspen digital team. Our theme music is by wonderly I'm Tricia Johnson. Thanks for listening