Cybersecurity Challenges and Opportunities for Small and Medium Businesses

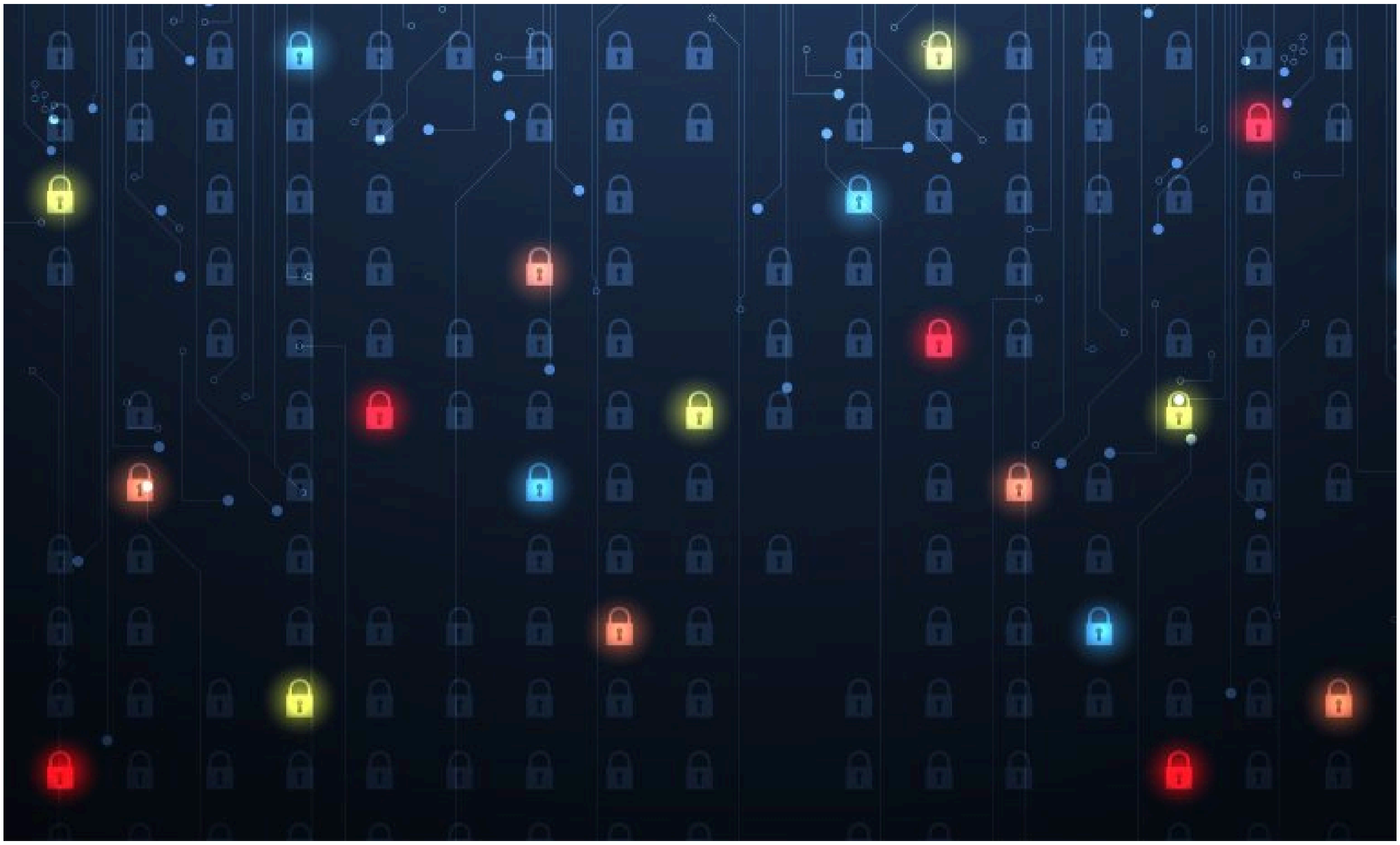

Photo: kras99/Adobe Stock

Transcript — March 9, 2021

Available Downloads

Download Transcript	243kb

Clete Johnson: Good morning, everybody. We are very glad to have nearly 400 people listening in now, and that number may grow while we're - while we're talking. My name's Clete Johnson. I'm a partner at Wilkinson Barker Knauer, and also senior fellow in the Strategic Technologies Program at CSIS.

I am very honored today to thank CSIS and Jim Lewis and the program for hosting what we expect to be not only an exceptionally informative event, but one that is incredibly timely with real-world operational response – operations underway right now with various high-level compromises and attacks that our country is grappling with. So we'll let our esteemed colleagues get into that more.

But we have – we are going to talk about the challenges for – and opportunities for critical infrastructure, small businesses. We're lucky to have the information security officer from one of those, Pioneer Telephone Cooperative, Chad Kliewer, on a – on a panel a bit later, along with the chair of the Communications Sector Coordinating Council, Robert Mayer, the newly installed executive assistant director of CISA Eric Goldstein, and the associate bureau chief for public safety and homeland security at the FCC Jeff Goldthorp; along with the CEO from CyberRx, who put this survey together, Ola Sage, who's also played a major leadership role in the IT Sector Coordinating Council.

But before we get to that excellent panel, I want to introduce and have a discussion with truly one of the – I think it's fair to say, one of the founding fathers of modern cybersecurity law and policy, Congressman Jim Langevin, who is the first and present chair of the House Armed Services Committee's new Subcommittee on Cyber, Innovation, and Information Systems. And he's also a commissioner on the Cyberspace Solarium Commission, which has enacted a number of ideas into law in the past year, and probably has more to do in 2021.

But before that, and on the point of Congressman Langevin's being a founding father of cyber policy, I want to go back to the 2008-2009 timeframe. I was a young staffer on the Senate Intelligence Committee working closely with Congressman Langevin's then-staffer Jake Olcott, who was one of our early fellow travelers on the Hill in cyber policy. And Congressman Langevin was the co-chair of – along with a Jim Lewis effort at CSIS – on a big report, a commission report for recommendations to the 44th president. That president turned out – became President Obama.

And a lot of the recommendations in that commission report from early 2009 are now policy. And they are the policy, and really the foundation of the policy environment we're navigating right now as we deal with SolarWinds, the other zero-day attack that has been in the news in recent days. And so I just want to start by saying, Congressman Langevin, we appreciate everything that you've done over the past really decade or more to establish a policy environment that allows us to respond to these challenges, and everything you're doing now on the – on the House Armed Services Committee, the Cyberspace Solarium Commission, and elsewhere.

So we're honored to have you. Welcome. And I don't know if you have anything to say before we get into questions, but I've got a lot of – I've got a lot of things I'd love to run through with you.

James Langevin: Sure. Well, first of all, Clete, thanks for the introduction. It's an honor to be here with you today and to see some old friends, particularly Jim Lewis from CSIS. And I want to thank CSIS for hosting this today, because, you know, under the guidance of Jim Lewis CSIS and Jim Lewis have been integral to my cybersecurity story, if you will. And that's how I really got started in this – in this field. Both – you mentioned Jake Olcott.

Jake, my staff director on the subcommittee that I chair that had jurisdiction over cyber, so it originally at least – the working threats cybersecurity and science and technology, and the emerging threats piece with all the bad stuff – which is what I thought we'd be preoccupied with – chemical, biological, radiological, and nuclear threats. I figured those would be the things that kept me up at night that we'd be doing the deep dive on, until Jake Olcott comes to me and tells me about this classified briefing I'm going to get on Idaho National Labs, and these two scientists who found out – who discovered the Aurora threat, as we now know it, that could cause physical damage through a cyberattack.

And so I began my deep dive on this. And then, of course, Jim Lewis asked Mike McCaul and I – my ranking member – to co-chair the Cybersecurity for the 44th Presidency – the CSIS Commission on Cybersecurity for the 44th Presidency. And we did this deep dive on cyber, on this topic. And it's – and it's really what launched me into this direction. And it's been a labor of love, although, you know, with great challenges along the way. But deeply indebted to Jim Lewis and CSIS for, you know, setting me on this path and for all the great expertise that they have brought to the table and brought to this issue of cybersecurity over the years. You'll see many of the – my subsequent work, whether it's, you know, in the caucus or now the Solarium Commission. You see a lot of the roots, the foundation of what we've done, coming from that CSIS commission, that report on cybersecurity for the 44th presidency.

So thank you; probably too long in my opening there, but I just want to express my gratitude and say a big hello to Jim Lewis.

Clete Johnson: Absolutely. Thank you, Congressman. And I think you just underscored how long you've been working on this. And I think we're at an inflection point now. And we're not coming to it flatfooted. We've got a lot of work to do. But I think we have the background of a decade or more of policymaking to address these challenges.

So let me just start with the focus on small businesses. This – the small businesses, and particularly critical-infrastructure small businesses, are at the heart of our economy and our society. You've – over the years you have been dealing with very high-level issues of Russia, China, Iran, North Korea, nation-state threats, the imperative of U.S. technology leadership and core U.S. national-security interests.

So what does all – what do those big-picture issues mean for these small businesses and the small-business critical infrastructure? Why does it matter to them? And why does that matter to us?

James Langevin: Yeah. So, you know, good question. Thanks for framing it that way, if you will.

You know, I think that it gets to the heart of something that I'm forever saying about cybersecurity. It's that it's not a problem to be solved. There's no such thing as perfect cybersecurity. We need to frame it in that way right off the bat. No cybersecurity is really – I'd say cybersecurity is really about risk management. If there's one thing I would want small-business owners to take away from my remarks today, it would be that.

You know, you're never going to install a device on your network one day or hire a service provider and then be able to forget about cybersecurity for your business. You look at cybersecurity, I'd say, as an ongoing process. So my advice to most small businesses – think about what your digital assets are and what it is you're really trying to defend. You know, there's some small businesses, for example, in my district that do very sensitive work for the Navy, so helping us – they're helping us build world-class submarines. So for them, digital assets might be their sensitive intellectual property. And for them, the threat from nation-states, particularly China or Russia, might be quite substantial.

But for most businesses, the most valuable digital assets for them are likely to be passwords to a bank account or customer information, and so – or, you know, maybe they rely on their IT to keep everything running day to day. So it's not risk to confidentiality that they're the most concerned about, but threats to the integrity or availability of the system. So for them it would be, you know, much more – they'd be much more concerned about cybercriminals than getting on the radar of Russia or Iran.

So cybercriminals, I'd say, are often in the volume business, looking into – where you cover up a lot of less valuable data or lock up computers that they might charge a couple of hundred dollars or a couple of thousand dollars to unlock. These criminals go after entities really with the weakest cybersecurity hygiene, which often unfortunately it means small businesses. And we've seen that too often. Ransomware is rampant right now, and it's hitting a lot of small businesses, in addition to hospitals or school systems.

So I guess that might seem like a lot of talk in Washington, D.C. is divorced from the reality of people back home. But I want to make something perfectly clear: Countries like Russia actively aid and abet cybercriminals. And that is one of the real frustrating things like that. And, you know, in other countries they're just looking the other way. You know, they don't care if cybercriminals are operating in their borders. If it's going after something that's targeted in the United States, what do they care? It's undermining our system, you know, our banking system or our business trust or business ecosystem.

And we're really living in a golden age of cybercrime because there are countries, again, that allow and encourage criminals to operate within their borders, and it's frustrating beyond words. So while some of the talk of norms and the need for stronger cyber diplomacy may seem esoteric, I can really assure you that it's increasingly relevant to stopping the constant stream of intrusions targeting small businesses around the country.

Clete Johnson: Well, I think that's the - all right. So that's a great segue into the next thing I wanted to explore with you, which is the concrete - this is not - you know, secure connectivity, as evidenced by this - by this Zoom event, is a - is an imperative part of our lives these days. Our kids are being educated online. We're working - we're teleworking, getting health care in the middle of a pandemic through telehealth, increasingly. And so this is a - this is a concrete reality for really all Americans. And a lot of that connectivity is delivered by small businesses like Pioneer, who we'll hear from in a moment.

So given that the bad guys, be it either cybercriminals or adversary intelligence services, are - we're on the good-guy side, we all of us - the U.S. government and industry - what can the government do, together with industry, to help? And you know, on this - on the next panel we'll have a number of key representatives - FCC, DHS, IT sector coordinating council, communications sector coordinating council. How do these entities - how can these entities support companies like Pioneer that are trying to keep our society connected?

James Langevin: Yeah. So I would say, you know, one of the key concepts in understanding Solarium policy recommendations is that of leverage. So the ability of malicious cyber actors to scale their activities is one of the things that makes cybersecurity problems so pernicious in a lot of ways.

On the Solarium Commission, therefore, we refocused on scalable solutions where a focused application of resources could have a big impact. You know - you know, while leverage is sprinkled throughout the report from the national cyber director to the very idea of defending forward or defending early, as my fellow commissioner Chris Inglis likes to say, really leaning into the point of high leverage, we acknowledge it most explicitly in the idea of cybersecurity enablers. So we touched on these things.

So cybersecurity enablers are, in essence, a new class of critical infrastructure. And since the Obama administration and Section 9 classification of particularly important critical infrastructure assets, you know, we've had the idea that not all critical infrastructure entities can be lumped in together. And so Solarium expands on Section 9 with our concept of systemically important critical infrastructure, or we call is SICI for short. I wish we had a better name, but that's what - that's what it stands for.

So SICI covers the assets that are most essential to supporting the national critical function set. But you know - you know, rather than view critical infrastructure as falling into two buckets - SICI and all the rest - Solarium realized that we needed a third category of entity that, while perhaps not systemically important, were the, you know, leverage points within the ecosystem. We need to treat these entities - the internet service providers, managed security service providers, and cybersecurity companies - differently, because when they take steps to protect their customers the whole ecosystem really benefits. And enhanced intelligence sharing with cybersecurity enablers, for instance, is much more efficient than trying to ensure that every company has the latest CISA alert, for example, and it's mostly the - results in the same level of protection.

So I'd say that, you know, building out the operational collaboration between government and cybersecurity enablers through programs like the joint collaborate environment is a key recommendation of the - of the Solarium Commission.

Clete Johnson: That's great. And with - thinking about managed services and - and you know, it's ironic that one of the - one of the best practices in cybersecurity, particularly for small businesses, is to seek third-party managed services and to make sure that their software is updated on a regular basis. And so this is something that's so troubling about the SolarWinds compromise, which is that companies that were using SolarWinds to do - to help with their cybersecurity that was actually the vector of the attack. So how do - what do we do - what do we do following SolarWinds to make sure that companies like Pioneer can continue to get secure third-party services and secure software updates?

James Langevin: Yeah. So, you know, this seems like a hard question but it's actually not. You know, we spend a lot of time telling people to update their software and then the threat actors abuse that mechanism to insert back doors, right. So I remind all businesses that the SolarWinds campaign was extremely sophisticated, and this actually goes back to the cybersecurity as a risk management exercise that I talked about earlier. You know, it took a lot of Russians a lot of time to execute the SolarWinds campaign.

So unless, you know, you're a small business with a lot of sensitive intellectual property or serve in the Department of Defense or intelligence community, my guess is that you're not on the Russians' target list and, you know, that's why my advice remains the same. That's to stay on top of your cyber hygiene. Many, many, many more people get breached due to unpatched systems than due to, you know, bespoke backdoors inserted into build processes. You know, now that software update has been exploited as an avenue of attack, you know, a lot more attention, obviously, is going to be paid to closing this particular door. It doesn't guarantee that it can't happen again, but you're far better off applying updates to remove zero-day exploits than postponing them.

Clete Johnson: I think that's – that is good advice. And with that, I want to close out by transitioning to the report that the panel is going to discuss right after our discussion. Of the critical infrastructure companies surveyed, 75 percent had experienced a breach, including 45 percent in the last year.

On average, it took almost eight months to recover from these breaches and an average of $170,000 to resolve the incident, which is, you know, big money for some of the – from some of the small companies. Nearly 60 percent reported that the incident stopped daily productivity and nearly half lost customers in the wake of the incident.

So I guess what I want to ask you is, first, do any of these numbers surprise you, and second, what's the value of a report and numbers like this for policymakers?

James Langevin: Yeah. So on the question of what's – you know, if anything surprised me, I'd say that, you know, 45 percent experiencing a breach in the last year seems high. But I'm guessing that, you know, some of that is how we define breach. So, you know, we're having these conversations today as we try to work out the specifics of when something crossed the line to an incident, you know, versus someone snooping around or doing port scanning.

So I guess I'm a bit disturbed that only 13 percent say they'd use government guidance. But I also wonder if that's the case, it's a case of this being the victim of its own success, perhaps. You know, after all, most of the cryptographic algorithms that we use are government standards. But I don't think a lot of people think of SHA-256 as being a government product. You know, we use it every day. So that's – I guess that's what, you know, kind of the things that stood out to me that maybe surprised me, if you will, or that really caught my attention.

You know, on the other question, you know, you had about the value of the survey for policymakers, you know, I think it's – I think it's an important reminder how pervasive these problems are and, you know, one of my colleagues on the Solarium Commission, Dr. Samantha Ravich, has been making the point that we too often fail to account for the human toll of cyber incidents, and whether that's the consumer victims of cybercrimes or the small businesses, you know, I agree with her that the conversations we have in D.C. can stray from the actual human cost of these breaches. And so surveys like this can help us better understand the full range of the ways that our constituents experience cybersecurity. And I think that they help us persuade our colleagues to prioritize cybersecurity on a national agenda.

I think, you know, the bottom line is that as much as, you know, we've been trying to, you know, up the awareness of cybersecurity over the years, the things that have gotten everyone's attention the most and have really hit home as a problem are the – are the – you know, the compromises that – you know, the targets of the world that compromise personal private information of customers that then, you know, people are up in arms. They, you know, get – they get back to their members of Congress and saying: What are you doing about this? Congress gets worked up. And then you have surveys like, you know, you put out that really helps us to understand the full scope of this and makes it real. So really invaluable work, and I'm deeply appreciative.

Clete Johnson: Well, thank you, Congressman. And thank you for your time. And again, not just your time this morning but over a decade of leadership on these issues. As I said in the beginning, I think we're – it appears to me that we're in an inflection point in both the operational and the geostrategic and policymaking environment on these issues. And I think it's – I think there's value in surveys like this, and also at the – you know, at the leadership and activities that you have underway on the committee and at the Solarium Commission, and beyond. So we thank you for your time and look forward to working with you in the coming months and years.

James Langevin: Thank you, Clete. You too. I appreciate you moderating, hosting me here today. And shoutout to, again, you, to CSIS, and especially to Jim Lewis. Thank you. Take care.

Clete Johnson: Absolutely. Thank you, sir. Thank you very much.

Well, I just want to thank the congressman for joining us here. And with that I want to turn the event over to another great leader in cybersecurity policy, this time working from the private sector. I've had the honor of working with Robert Mayer in his role at USTelecom and also in his role leading the Communications Sector Coordinating Council, for about as long as I've been watching the leadership of Congressman Langevin.

And I will say that – whether it's working on the FCC's advisory committee, the CSRIC – I won't even go through that acronym – but the leadership that Robert has shown in that capacity, on the supply chain task force, and in a whole host of issues fighting botnets and establishing the Council to Secure the Digital Economy. Robert is also one of the most influential leaders in this arena.

And I will give him the honor of introducing his esteemed panel. It is another great group of leaders. And, like I said, I think sort of a microcosm of the solution set – FCC, DHS, IT Sector Coordinating Council, Communications Sector Coordinating Council, and then in the form of Pioneer Chad Kliewer, one of the small businesses that's keeping our society connected.

Robert, over to you.

Robert Mayer: Oh, great. Thank you, Clete, for those kind remarks. And thank you to CSIS and Jim Lewis for hosting this event and giving USTelecom an opportunity to talk to such distinguished panelists as we have here about the critical infrastructure small and medium business survey that we conducted. I'm just going to do a quick introduction because all of these folks really deserve the same kind of laudatory remarks you made for me. They're all leaders, and it's been a real honor to work with each one of them over the years.

Ola Sage describes herself as an entrepreneur at heart. She's a recognized leader in cybersecurity, a CEO of CyberRx. She leads an organization with a particular focus on cybersecurity for small and medium businesses. Ola and CyberRx led the research efforts associated with the USTelecom SMB survey that we discussed today.

Chad Kliewer is the information security officer overseeing the cybersecurity, privacy, and IT governance programs for Pioneer Telephone Cooperative based in Kingfisher, Oklahoma, and a member of USTelecom. He has over 20 years' experience in information technology with responsibilities ranging from PC tech to chief information officer, and most of that time being the primary person responsible for security.

Jeff Goldthorp is the associate bureau chief at the Federal Communications Commission. His role in the public safety and homeland security is chief data officer and national security policy. Jeff has been involved in numerous cybersecurity initiatives with industry through his prior leadership on the FCC's Communications Security, Reliability, and Interoperability Council, CSRIC.

Eric Goldstein serves as the executive assistant director for the DHS Cybersecurity and Infrastructure Security Agency, CISA. In this current and recently appointed role, he leads CISA's mission to protect and strengthen federal civilian agencies and the nation's critical infrastructure against cyber threats. Eric returned to DHS with the new administration, and our sector is looking forward to advancing the partnership we have with DHS as our sector-specific agency.

We're pleased to have all these panelists today.

Now to the report. Real quickly, USTelecom commissioned the report last year, conducting the survey several months after the pandemic changed all of our lives. CyberRx interviewed 14 CEOs and senior-level executives for a qualitative understanding of their perspectives around SMB Cyber and their organizations in particular. This was followed up by a detailed survey with 323 responses across multiple critical infrastructure sectors including, for example, financial services, health care, critical manufacturing, information technology, and communications.

OK. Before we get into some of the specifics, I want to ask you folks the same question that Clete asked the congressman. You've had a chance to look at the report and read it, and I'm wondering if you can share with us what you found as the most surprising results of the – of the survey, perhaps what you would not have expected, either a particular finding or more generally across the findings of the report. And let's start with – maybe I'll ask Ola to begin.

Ola Sage: Good morning. Thanks, Robert. And I just also want to add my thanks to CSIS for hosting this event and to USTelecom. We were really grateful and appreciated the opportunity to be a survey partner on this really groundbreaking study that was primarily focused on just critical-infrastructure SMBs.

There were so many things that were of note in this survey, so it's hard to pick one. But I think the one that I would probably start with was just what kept coming through was this relationship between the size of an organization and their experiences with cybersecurity. So whether it was the amount of time it took to recover or how much money they spent or their exposure to attacks, that was something that really stuck out to us and something that I think we would love to learn more about because that could also influence various kinds of policies and guidance that we use going forward.

Robert Mayer: OK. Thank you.

Chad?

Chad Kliewer: Thanks, Robert.

And I have to say that part of the report that really surprised me in there and still perplexes me just a little bit is the part where it talks about which – how comfortable you are with your information security, how secure your company is. Starting with the smallest companies, they're pretty sure of themselves. In the middle, not so much.

And then once it got to the larger companies, they're more sure of themselves again. And I thought that was really telling, and it makes me wonder: The smallest companies, do they really not know what the threats are out there, or are they really that confident that they're secure? So I thought those were some really interesting numbers that came out of this.

Robert Mayer: OK.

Eric?

Eric Goldstein: Thanks, Robert. And just echoing the other panelists, thanks to CSIS. And of great importance, thanks to Mr. Langevin for his decades of leadership in this space and for the Solarium Commission's work in really advancing the state of the cybersecurity discourse in this country. Certainly, we at CISA are deeply grateful for the congressman's work and that of the commission.

You know, I really share Chad's observation on the report, which is I remarked upon the surprisingly high number of companies across all tranches of the study reporting very high confidence in their cybersecurity protections. And I think this is a time, particularly given the ongoing intrusion campaigns that we're seeing in this country, when all companies and all organizations need to be taking a deeply self-reflective look at their cybersecurity controls.

I will just call out of particular importance the ongoing vulnerabilities and intrusion campaign targeting Microsoft Exchange servers, which affect companies and organizations big and small throughout our country. I would just take this opportunity to encourage any attendees at this panel, please do urgently look at guidance that my agency, CISA, has put out to mitigate this vulnerability. It is an urgent national risk and I think reflects the fact that, big or small, all organizations face significant cybersecurity risks and need to prioritize controlling those risks accordingly, whether doing it in house or with a third party. We are past the days when SMBs or large companies can not be in the business of cybersecurity. Every business leader needs to see cybersecurity risk as a core function of their business risk management.

Robert Mayer: OK, very good. Thank you.

And Jeff.

Jeff, you are on mute.

Jeffrey Goldthorp: Thanks, Robert. I was having some difficulty getting unmuted. (Laughs.) Thank you.

And thank you to USTelecom and to CSIS for having us on the panel today. It's a pleasure to be here.

And let me offer some thoughts about the question that you asked. First of all, the report that you all issued, I thought, was very good. And there were some really good insights there. One thing – I will share something that the congressman observed is the relatively low percentage of respondents that were using guidance from various federal agencies in their cyber-response efforts.

And I think the words he used were that maybe we're a victim of success there in some ways. I think there are some things we can do to improve there. And we can probably talk about those some more later. We've got some – I've got some ideas I can share with you. There's some work going on in the task force that you're co-chairing, Robert, that might be helpful there, and some work that's been done over the years in CSRIC that you were involved in that could contribute.

Something else – and this is a little – this was surprising to me – was what appeared to me to be the relatively low incidence and low cost of cyber events affecting respondents. And now I think that there could be interesting discussion about this, because I think, depending on your point of view, you might say, well, if you're a small and medium-size business, you don't have a whole lot of money to spend. So, you know – but still, when you take the numbers from the survey and you run through the expected value, you come up with a figure that isn't super high. And that surprised me.

So that I just wanted to throw out as something that has sort of caught my eye.

Robert Mayer: Yeah.

Jeffrey Goldthorp: And I'll turn it back over to you.

Robert Mayer: Sorry to interrupt. Jeff, I think you make a great point about the costs and the benefits, you know. As indicated by Clete earlier, average – companies spent on average $170,000 to recover from a breach. Forty-six percent claimed that they had lost customers as a result. Fifty-nine percent reported that they had the incident that stopped daily productivity. And it took as much as seven and a half months to fully restore.

So there is a big cost. And then you have to match that – and again, that's an average number, so it varies by size. But you'd have to kind of take that as the cost and then think about what it would cost perhaps to mitigate that. And I think you probably will find some cost-effective price point in which to invest in cybersecurity.

The report states that, quote – and I'm quoting here – critical-infrastructure SMBs with $50 million-plus in revenue indicated that they use and place a great deal of importance on nearly all best practices assessed in the survey. Conversely, organizations with less than $1 million revenue are more likely to report placing a lower level of importance for a majority of the best practices than SMBs with more than $1 million. Respondents were asked about their use of specific best practices, such as multifactor authentication, training, policies and procedures, risk assessments, insurance, and software updates.

I'd be interested in knowing your thoughts on the implications of this finding, and more specifically what you think are the biggest obstacles to raising the cybersecurity posture across many critical-infrastructure SMBs. So who wants to volunteer and take that first? Otherwise I'll –

Ola Sage: I'll take a –

Robert Mayer: Thank you, Ola

Ola Sage: I'll take a stab at it.

And, you know, this is something that was of interest. Our lead researcher, Dr. Williams, was really – this was something that struck his attention as well. And, you know, the explanations could range anywhere from, you know, perhaps these SMBs have this sense of invincibility in that they feel like perhaps they're less of a target because their revenue is not high, and so maybe they don't feel that there's as much of a priority in terms of investing in some of these interventions. But that's something that we want to understand more.

I also quickly just wanted to add some context to that 13 percent, because I think that the way it was asked was how are they using it to make decisions, right. So it wasn't really reflecting that they didn't read the guidance or value the guidance. It was how are they using it to make decisions. So we were actually a little pleasantly surprised to see that over 10 percent were actually using, you know, federal or government information to make decisions. And certainly we want to see that number increase, but as a starting point it was something that was, we thought, a positive, net positive.

Eric Goldstein: Hi, Robert. I'll also offer a view here, if I may, just on the broader question, which is how do we further incentivize or encourage investment among SMBs in this critical area?

And I think one important framing point is that, you know, adversaries of all types are targeting American businesses now. And it is not just the case that if you are a company that has highly sensitive IP or provides critical infrastructure that you're the only type of company at risk. We are now seeing adversaries, including criminal groups, that will launch what I call indiscriminate attacks, really just targeting anybody in this country with a vulnerability in order to launch ransomware attacks, extort money for information, those kind of activities.

And so really every company in America is at risk. And, you know, even if the services provided or the data stored by a given company wouldn't seem to be of interest to adversaries, that's simply not the threat activity that we are seeing across this country. And so every executive should see themselves as being at risk and take urgent steps to manage vulnerabilities in their IT infrastructure, whether they're providing it themselves or contracting with a third party for those same services.

Robert Mayer: And Eric, we're going to get to that point about executives next, but thank you for that.

Jeff, do you have some thoughts on the results and what the –

Jeffrey Goldthorp: Yes.

Robert Mayer: – implications are?

Jeffrey Goldthorp: Yes, I do. Thank you, Robert.

I think the – one thing I would suggest, one of the – you were asking what can be done to help better prepare. And I think that if I were a small and medium-size company and looking at the volume of guidance and practices – and I'm thinking now specifically about the commission, right, and you're familiar with the work that CSRIC has done. There are 400 cybersecurity-related best practices that CSRIC has recommended to the commission and that we've made publicly available. That's a lot.

If you're a tier-one communications provider, that may be something that you can absorb and you have the staff to apply and you've got the resources to apply. If you're a small communications provider taking that number of practices and figuring out which ones are the most important and which ones to spend money on is challenging. And even finding somebody to go through 400 things – (laughs) – and making that decision can be challenging.

So what occurred to me is that – and I think this is something that you and task forces are thinking about as well – is what can be done to take the guidance in various forms from CISA and from FCC, from NIST, and boil it down into something that is more that can be applied in a more practical way by smaller companies, not just communications providers. But that to me would be a useful outcome.

Robert Mayer: And you have one of the co-chairs of a new task-force group on small-medium business. So Ola –

Ola Sage: Yes. Yes, absolutely. And just to build on that point, I think this boils down to – you know, our friend Larry Clinton, right – the economics of this, right, for most small and mid-sized businesses, how can we make it economically viable for companies of all sizes to invest? And how can we move this up on the prioritization list, right, so that it becomes a higher priority, and it's – and it's more economically feasible?

Robert Mayer: Yeah. A great segue to you, Chad, since you have to live with the economics of security every single day. How do you prioritize? How do you think about making the case to your management about resources and determining what's most critical and what assets are most essential? What's the – what's the process like? You can talk an hour for that. You've got a minute or two.

Chad Kliewer: Yeah, you're exactly right. It could easily take an hour. But, you know, number one, the first thing I try to do is – even though I'm a technologist at heart, I have to try to take the technology out of things. We have to think like the business and really elevate information security and cybersecurity to the business level. It's not a technical problem. It is a business issue. And the first thing that we have to do there – you know, of course, we can't implement all 400 and some of those recommendations. There's just no way you can do that in a small or even a medium business. Even a large business would probably have challenges with that.

So what we've got to do is figure out – you know, the first conversations I had here at Pioneer is where are the crown jewels. What are we trying to protect? What – you know, where are our vulnerabilities? What's our biggest step? And you know what we found here? Our biggest – our biggest assets are, number one, the network availability. That's number one for us. And then, of course, number two is our reputation or our integrity. So those are where we have to concentrate our efforts. So we have to make sure that everything we do as part of an information security program is trying to align with those business goals and make sure that we're, number one, protecting the availability of our networks and, number two, protecting the integrity of those networks and the accounts that are around it.

Now, that's not to say that we completely ignore the other parts of it, because confidentiality of course is a very important part. But the confidentiality part does not play quite as big a role if we can't provide a network.

Robert Mayer: Yeah. Yeah, to your point about business, I think that's what motivated USTelecom to set up a partnership with the American Small Business Development

Centers. They have 4,000 centers that are now working on developing a cybersecurity program. But, to your point, in the language of their businesspeople, not so much in terms of operations and technology, so they get more comfortable with it.

I'm going to – I'm going to move along. I want to point to one of the findings in the report that I think may be a little bit concerning. That is the discrepancy between the board and C-suite views on cybersecurity as a high priority, versus the lower echelons, the employees of an organization. I think the distinction was 50 percent view it very high at the – at the very top management level, versus 26 percent at the employee level. And I want to know what you think – what do you attribute that kind of disconnect? And most importantly, what needs to happen internally within the enterprise and externally among stakeholders to narrow that gap? Who would like to take that?

Jeffrey Goldthorp: Robert, I'm happy to –

Robert Mayer: Yeah, go ahead, Jeff.

Jeffrey Goldthorp: One thing that I noticed in the report is that only 40 – well, I say only – but 42 of the smallest respondents made use of sort of educational, you know, supplements after an exploit. And that's the sort of thing that would seem to come at a relatively low cost. And so, you know, if you're going to do something, that's something you can do. And it's, say, on the low end of the – of the pain curve. So that surprised me. And it also would, I would think, lead to a – it would – if there were more education, more awareness, more training being done – especially after an incident like that – then you might have seen a different outcome in the survey.

Robert Mayer: OK. Very good. Anyone else want to comment?

Chad Kliewer: Yeah, Robert, I'll jump in on that one just a little bit. You know, I think it's education – it's all about education. And it's all about empowering the workforce. I was – I was not that surprised to see 50 percent of executives count it as a high priority. It's – let's be honest, it's not a money maker for most people. You know, we're a place where you throw money and watch it go down the drain, although we're doing good work for it. Don't get me wrong there. But you know, it's not a money maker for companies. And that's why it harder for companies to see.

The other side of that is the employee part. And that part, you know, I have to say, that part hurt me. I spend a lot of time - I spend most of my time concentrating on the employees and on the workforce in making sure that everybody in the workforce knows that they are a part of the cybersecurity team here at Pioneer. And that's what it's got to be. I hear too many times, oh, the antivirus protection will - you know, the antivirus will protect me from that, or so-and-so will protect me from that, or the stuff you do, you know, you'll protect us.

And the fact of the matter is, no, I can't protect everything. And that's why I have to make sure that everybody knows that they are a part of the solution. And it's more - we talk about partnerships. We talk about partnerships at the industry and government level. I build those same types of partnerships right here in between departments, in between individual people to make sure everybody knows we're all partners, we're all in this together, and there's not one of us going to protect it.

Robert Mayer: Mmm hmm. Ola, can I ask you maybe to comment? I know you work with companies at the executive level, so you have a good appreciation, I think, for what their awareness, heightened awareness or lack thereof, is, versus employees. What can you - what do you see broadly across the SMB spectrum?

Ola Sage: Sure. So here I kind of wear two hats. One is, you know, CEO myself of a small, mid-sized business, and what I've seen over the years in my own companies. And then as a practitioner, right? And I do think that the gap was striking. So from the CEO hat perspective, I would say, you know, every company values - you know, what the top of an organization values is what the company ultimately will value. And perhaps even more - you know, more significantly in smaller organizations, where you don't have thousands of employees, et cetera.

So there are a couple of explanations, but I think this is definitely something that we would love to explore more. It could be anything from the executives just have more access to this information and so they're more aware and informed about cyber threat, and therefore they value it more. And it could also be that even though they value it more, there are not internal mechanisms within their companies to get that information to the employees, right? So whether - they may not have programs in place, or they may not have opportunities or mechanisms for the employees to get access to the same information they have.

On the employee side, it could be as simple as they just feel like it's somebody else's job, right? It's the job of IT. It's the job of the company. It's not their personal responsibility, which still brings us back to this education and awareness question. So it was striking. And I think there are opportunities there to understand better what that's about, so that we can figure out how to close that gap.

Robert Mayer: Mmm hmm. Eric, I know you're - you've got some time constraints. Are you still there, Eric, or did we lose you already? We may have - Eric is doing the lord's work at DHS right now, so understood.

Let me - let me start probing on a couple of things that I think go to managing expectations, frankly, of companies in the small and medium business size. And I think this is particularly relevant in thinking through current policy and also future policy. And I'm glad Ola that you mentioned our friend Larry Clinton because over the years I've become a disciple on many of his points, and especially the notion that this is an economic problem at its heart.

So given that many of the most recent attacks, the highly visible ones, you know, are conducted by criminals - you know, organized criminals, many of whom are in partnership with certain governments, nation-state adversaries. And there are two in particular that are capturing headlines right now. I think it's important to think about what is the government's role in protecting SMBs, and more broadly industry, from those kinds of attacks? And what is the industry role? And how do you - how do you parse that? How do - how do you work through those - that balancing act?

Who would like to start with taking that? Jeff, I can ask you to think about that, maybe to start with us, because, obviously, in the government you have to think about making sure there's accountability and that there is progress in this area. But you know, as Larry said, you know, the varsity team missed SolarWinds. And it was sitting there, I don't know, for eight months or longer without it being detected, and it was the private sector that detected it. How do you think about a small and medium critical-infrastructure company – a water company in some city in Ohio, very limited resources, you know, looking at its rates, looking at its customer base and their ability to pay – how are they supposed to defend themselves against those kinds of attacks?

Jeffrey Goldthorp: OK. Thanks, Robert. Let me – you said you'd give me some time to think about this, so I'll take give seconds. (Laughs.)

Robert Mayer: Absolutely. Take longer.

Jeffrey Goldthorp: (Laughs.) OK. But I will take a moment because that's a serious question. Not that you – you know, all the questions you've asked are serious. That's a hard question.

So one of the things that the congressman mentioned was using, you know, essentially cybersecurity insurance and third parties, OK, so using other stakeholders that are participating or contributing to provide solutions, right? If you are a small- and medium-sized business, that is something to consider because you probably won't necessarily have the means to do it all yourself. So relying or finding the right partners that can help you compete effectively is one way to do it. And those two – those two segments or those two categories of players are two that I would consider.

You started your question by asking about the role of government, right? Am I right? Is that –

Robert Mayer: Yes. Yes.

Jeffrey Goldthorp: OK. And so I think that different agencies will answer that question differently. CISA will, obviously, have an answer. They're the sector-specific agency for communications, as well as other critical sectors. And NIST has a – has a major role to play in establishing standards and guidance in this area. FCC, the regulator, has a role to play.

And the good news is that, as you know, I think – and hopefully you'll back me up – there's been a really outstanding teaming relationship between those three agencies over the years in this space. And that applies to the work in CSRIC IV that you were involved in, Robert, and it applies to other elements of work. So the fact that there's good teaming between the agencies that have a direct role to play is helpful.

I think that what would be even more helpful and something we can work on going forward - and maybe with the benefit of the work that the taskforce is about to start - is to - is to try and apply what can be a fairly robust and rich and large - (laughs) - set of guidance and practices to a - to a sector or a segment that has a different set of needs and where the scale is smaller. So, now, that is - there has been an effort. There's been some work like that done in the past that Working Group 4 was involved in back in the day. This has been several years now. But I think the work that the taskforce will be doing will be really helpful in bringing together the FCC and the other agencies that have a role to play in this in trying to build solutions that are - that take what the government is having - has to offer for what are the larger entities and make them more useful to the types of firms that we're trying to reach on this - in this venue.

Does that answer your question, or have I -

Robert Mayer: I actually found your response exceptionally thoughtful, and I think the points you raise are important and need to be followed up on.

For the benefit of the audience who may not know, the references to the taskforce refer to the Department of Homeland Security ICT - Information and Communications Technology - Supply Chain Risk Management Task Force. That's a long title. We never figured out a way to make that a little smaller. We are now starting a third program after two years of reports. And one of the points that we're interested in doing that we will do is taking the products that have been developed over two years on supply chain and making sure they're not sitting on a shelf and nothing happens with them. So the work - the taskforce is actually working now to make sure that the best practices and the insights that came out of all of that analysis get - become available and get adopted and understood by members in this ICT sector and in particular, importantly, for SMBs.

Does anybody else want to respond to the question I posed to Jeff regarding the distinction between dealing with attacks that are, you know, global and highly sophisticated to the point where even the best organizations on the planet are struggling to keep up with them, and how small businesses have to position themselves in this kind of environment going forward?

Chad Kliewer: I can take that, Robert.

I think the important thing to remember - and you know, part of me says - as much as it pains me to say, you know, part of me says it's really great that we're seeing this kind of press on some of these huge - on some of these huge breaches that are out there. You know, it does bring cybersecurity more into light. It definitely brings it to top of mind for a lot of folks.

The thing to remember, and especially about the SolarWinds breach, there was some very, very sophisticated stuff going into that in establishing that backdoor that was done by, you know, a nation-state. The thing is, though, is once they established that backdoor and once they got their foothold in an organization, they weren't necessarily quiet moving around, doing what they were doing. So those that started from the basics and really started building their security programs using those very basics - the two-factor authentication, making sure your employees have training, making sure your software's up to date - that stuff really played a huge role after that foothold was gained and stopped them from going a whole lot further in many - in many organizations. You know, they still were able to get too far in a lot of - in a lot of, I guess, high-value organizations, but some very basic cybersecurity hygiene stopped them from a lot of organizations.

Robert Mayer: Mmm hmm.

Ola?

Ola Sage: Robert? Sure.

I was just going to add a thought. I think, based on kind of what I've been seeing and experiencing, I couldn't agree more that we're going to need both sides, right, government and industry. And these partnerships, whether it's the ICT Supply Chain Task Force or other public-private partnerships, I really think are going to be a huge part of the - you know, the solution going forward in terms of how to deal with these things. And I think that in some areas the government will lead and then in others the private sector should lead or will need to lead.

The National Infrastructure Advisory Council just published a report about actionable cyber intelligence, right, and it's an executive-led collaboration model about how to potentially establish what – this was called a critical infrastructure command center. And the goal of this particular solution is essentially to create solutions products that can be deployed quickly to large and small companies to help them understand in a much faster way kind of how their systems or infrastructure may be exposed. So it's things like that that I think that, you know, government and industry working together to actually come up with actual actionable solutions will really make the difference.

Robert Mayer: OK.

Looking at the time, so I've got one more question, and want to – it's kind of self-serving. But if we were going to do a survey again, what would you like to see us explore based on what we learned from this first effort? Where can we improve the information?

So, Ola, I'll start with you. Maybe you have some thoughts on this. I'm sure you do. You know, where can we probe to get some even more important and actionable insights?

Ola Sage: Well, I'll start with something the congressman talked about when he mentioned some of the things that caught his attention, and particularly the 45 percent who experienced a breach in the last year. And I think one of the things that was interesting to us was, you know, it's been clear about the distinction between attack and breach, but how different companies interpret what is a breach. Is it just disruption? Is it damage? Is it theft? Is it unauthorized access?

I think those are areas that we want to potentially explore a little further. So we're all talking about the same thing when we say breach, because that was a fairly high number as well. And I think, going back to my original comment about this relationship between size of organization and their experiences with breach, I mean, we found that, you know, 11 million (dollars) to – I think there was 20 million (dollars)