THE NEW BATTLEGROUND FOR TECHNOLOGICAL DOMINANCE

HOW CYBERSECURITY PLAYS A ROLE IN POLICY

Published May 2021

Executive Summary

Since the turn of the century, we have experienced a new age of connectedness, and with it, increased cybersecurity challenges. Cyberattacks of massive scales like the ransomware attack on the Colonial pipeline[1] and the Solar Winds and Microsoft exchange breaches have revealed vulnerabilities that Congress has attributed to "a collective failure" to prioritize cybersecurity as a pillar of national security strategy.[2] Furthermore, cybersecurity experts have warned that tech security should be contextualized as the clash of two opposing visions on how to use technology-one as open and free and the other, digital authoritarianism, to control and coerce.[3]

In our 2020 research, we talked with policymakers in Congress, the executive branch, and the private sector who provided organic anecdotes about cybersecurity and other aspects of tech security. In addition, they told us what they want to hear about from companies and associations on these issues.

Cybersecurity

Despite the pandemic, interest in cybersecurity increased among policymakers on both sides of the aisle who want to hear about how stakeholders across industries are addressing security concerns.

The National Security Link

Policymakers are faced with multiple issues at the intersection of technology and national security, including digital authoritarianism, data sovereignty, and securing supply chains.

The Case for 5G

Policymakers and experts view 5G deployment as a way to secure supply chains, advance an open and free use of the internet, as well as usher the next wave of technological innovation.

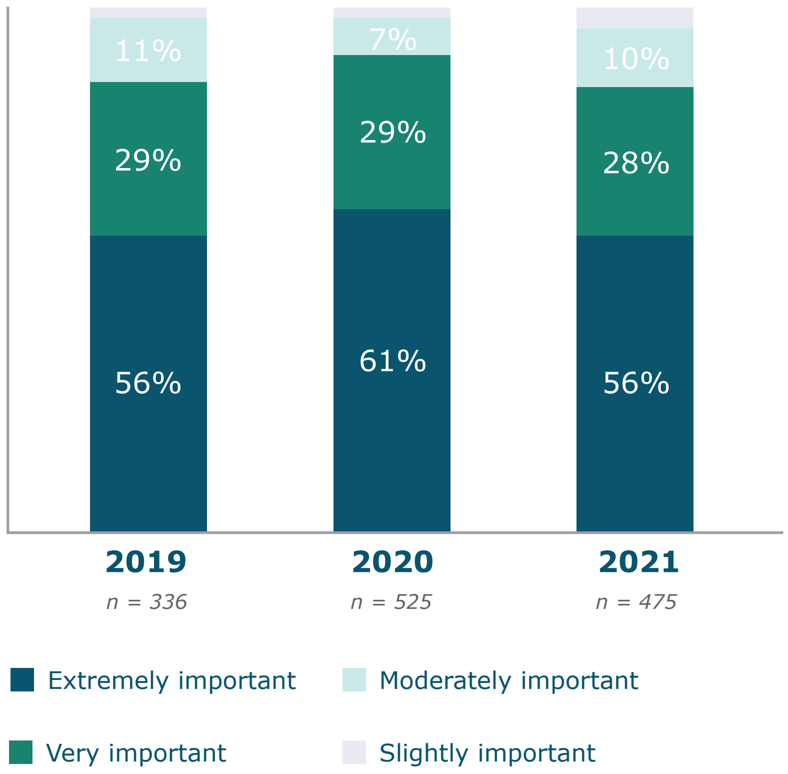
Tech Advocacy

Policymakers want to hear about what companies and associations are doing to strengthen cybersecurity. Information sharing, from basic to advanced, is welcomed and expected to be ongoing as threats change and adapt.

Cybersecurity

The percentage of policymakers who consider cybersecurity extremely important remained high from 2019 to 2021

"How Important Are Cybersecurity Policy Issues in Your Opinion?"



84% of policymakers think cybersecurity is extremely or very important

<1% of respondents chose "not at all important" in each year of the study

Every year we've studied the topic, a majority of respondents have identified cybersecurity policy issues as extremely or very important.

*" I would like to see greater signaling of a commitment to cybersecurity than we have in the past... **To me, it's not a partisan issue. It's very much a national security issue.**"*

-Senior Advisor, Executive Agency, R

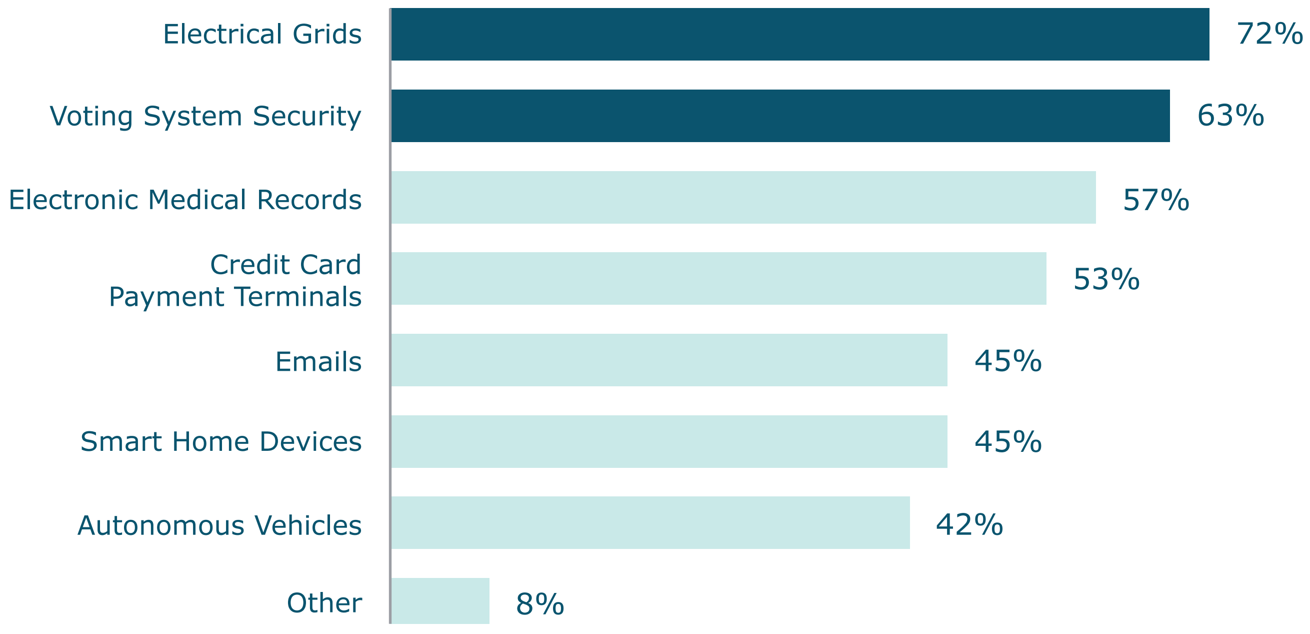
*"I think there's more consensus on-- there might be a lot of different opinions, but I think **there is more consensus there [on cybersecurity] than there is on privacy.**"*

-Vice President, Government Affairs, D

Cybersecurity

Over 60% of policymakers surveyed in 2021 viewed electric grids and voting systems security as areas that require stronger government standards

"Which of the following do you believe require stronger government standards to prevent cyberattacks?"



n = 472

The Washington Post

Fuel shortages crop up in Southeast, gas prices climb after pipeline hack

In our 2020 conversations, policymakers expressed concern over disruptions to critical infrastructure in the event of a cyberattack. The Colonial Pipeline shutdown and its effects on the economy and day to day life confirmed their concerns.

> *"Cybersecurity is a huge issue and a huge matter of concern.* ***I know that foreign governments have already shown an ability to access critical US infrastructure that could really shut down economies, the way of life for long periods of time.*** *So I think it's very, very important."*
>
> -Senior Staffer, House of Representatives, R

The National Security Link

Cybersecurity is part of a broad range of issues policymakers are grappling with at the intersection of technology and U.S. national security

As countries set the tone on how to use technology, what rules to follow, and what values to answer to, two different visions emerge; open and free or controlling and coercive.[4] A variety of issues surrounding this theme emerged in our conversations with policymakers.

Digital Authoritarianism

Digital authoritarianism is the term used to describe a state's use of big data and technology for autocratic purposes, and it is on the rise with several nations perfecting and exporting this model. Policymakers expressed concerns about adversaries using technology to limit freedom and repress populations.

"The thing that I would flag front and center on tech... is the rise of what we call, digital authoritarianism. And it's basically ***this model that China is perfecting by using technology to sort of control and repress their population.*** *And the Chinese have been-- they've been exporting this. They are perfecting it. They are exporting it around the world, and other countries are eager to follow."*

-Senior policymaker, Legislative Committee, D

Data Sovereignty

The location where data is stored has implications for national security. Our research showed policymakers have questions about where companies and products store data, and how that information is used by countries that may have antagonistic relationships with the United States.

"The biggest problem is where is the data stored? Who has access to it?...Is it going to some Chinese products somewhere? And that's a concern because of obvious reasons. And so that gives them an advantage... That's the issue. Those are the things that I think are most concerning these days. It's just easily broken encryption or ***data that resides in places that don't share our values and worldview."***

-Senior policymaker, Senate, R

Technology Supply Chains

"A bigger push I've seen has been with the hardware side, ***lots and lots of interest in making sure that we are not using the same chips that are being fabricated elsewhere that might be contaminated or compromised in our secured systems here in the States that might cause us a problem later,*** *especially for critical infrastructure things like power plants, utilities, classified environments, those kinds of things that there's case studies that actually show, hey, you can't trust the hardware that's coming out of these areas."*

-Defense Policy Expert, Senate, D

The Case for 5G

5G technology brings faster speeds and galvanizes innovation as we become increasingly connected to the internet.

In light of concerns over supply chains and digital authoritarianism, calls for investments in 5G deployment in the U.S. and other democratic nations get louder. However, there is uncertainty about how to fund it and how to make it affordable for rural customers.

*"**We're going to see just a flurry of innovation that's going to be driven off this 5G platform.** US policy is going to be pretty clear that we're going to want to **invest and grow as fast as possible because it's to our economic advantage.**"*

-Legislative Assistant,
House of Representatives, D

*"Everyone is focused on dealing with COVID-19. In the meantime, you've got the 5G question, **what do you do about 5G?** The residual is going to be, at least people I talk to on the Hill is, 'is this going to be an avenue to do something with 5G infrastructure which will actually be good for jobs and the economy?' **But no one knows how to pay for it.**"*

-Associate Director, Think tank, I

But, according to Brookings[5], **the distributed nature of 5G makes it more difficult to address security concerns from a central point**, creating cybersecurity vulnerabilities that can be exploited by bad actors. Allowing 5G infrastructure from companies like Huawei, which have a lower price due to heavy Chinese government investments, can therefore result in additional risks to the U.S. and other countries.

*"We have enough problems with getting rural internet to every single American. Now, we can get real internet including 5G for every single American. And **Huawei has a very attractive price. And now we're telling them, "No, you can't use them." So we're basically just trying to pump up our domestic capacity to be competitive at the price level.**"*

-Legislative Assistant, Hill, D

*"The future of technological innovation is reliant on 5G. I don't think there's a lot of confidence right now that there is a US producer who can sort of establish a broad 5G network in the States. So now, they're trying to cobble together what the Europeans can do because **we want to stay away from Huawei and their 5G capabilities.** I think the 5G...rollout just began, which is promising. I think it's yet to be seen whether it'll happen on a wide scale."*

-Policy Advisor, House of Representatives, R

Tech Advocacy

1

Policymakers, especially Hill staff, welcome information on topics related to cybersecurity.

“Companies should proactively reach out to congressional staffers and say, ‘Cybersecurity is an issue and we’d like to hop on a call with you for 30 minutes and tell you about it.’ ***If people call and say, ‘We can educate you and offer you a briefing on this topic’, most people are going to want to pay attention.”***

-Professional Staff Member, House Committee, D

2

Policymakers are looking for increased information-sharing between the public and private sectors to keep abreast of potential vulnerabilities for companies, vendors and supply chains.

“You’re allowed to pass costs on to ratepayers. ***That’s why we want IOUs to talk to policymakers to demonstrate that they’re taking this seriously, and have them be part of the conversation of what it takes to do it effectively.*** *They know their own businesses and operations better. We want to know when third-parties are involved in the provision of these services and where those third parties are. Make sure that there’s security there.”*

-Senior Staff, DHS, R

3

Cybersecurity will continue to be a moving target. As security improves, new threats will appear. Policymakers want to know how companies are protecting their systems now, and how they are anticipating the next threat and continuously investing in security.

*“****The fact that things have gone well with cybersecurity in the past does not really give that many people in the agency confidence that they’re going to continue to go well in the future.*** *Cybersecurity is one of those things where it always feels like you have to keep moving and you have to keep improving because all it takes is one slip up for things to go horribly awry.. I know that the* ***people I’ve worked with have been far more impressed by people setting up systems*** *that make that kind of stuff literally impossible to happen rather than being impressed with people saying, ‘****Hey, for the past 80 years, nobody’s hacked into our system.’ Okay. Well, that doesn’t mean no one’s going to do it tomorrow.****”*

-Senior Staff, DOE, D

Learn More About The Ballast Policymaker Hub

An Exclusive Invitation to the Ballast Policymaker Hub

Why Join The Ballast Policymaker Hub?

The Ballast Policymaker Hub provides data-driven insights and resources for those in the public sector, including:

- Career development resources and guidance
- Invitations to events led by seasoned policy and private sector leaders
- Research insights on advocacy efforts, based on feedback from senior policymakers
- Opportunity to participate in pioneering annual research

Participation is open to those currently on the Hill and to policy experts in the White House and Executive Branch agencies. There are no fees or time commitments.

Our Goal

The goal of the Ballast Policymaker Hub is to offer unique value and insights to policymakers, who are instrumental in our efforts to further public and private sector collaboration in the advocacy space.

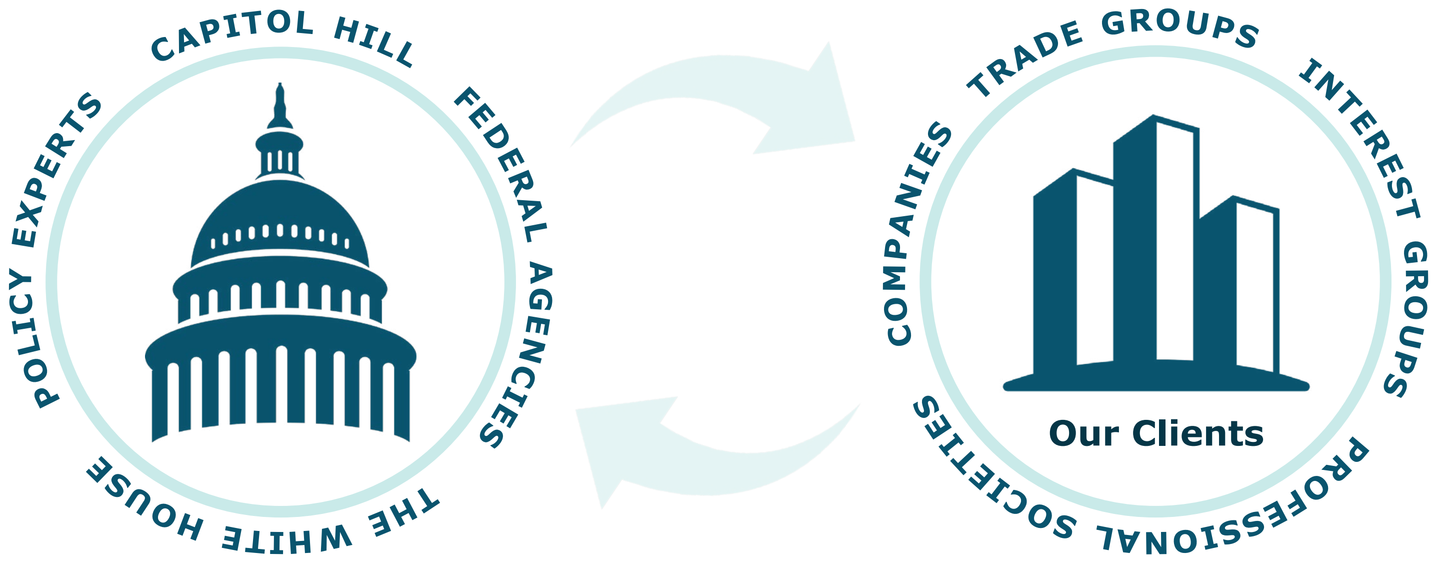
> *"We, as a government, never want to just be dictating to these companies what's happening. We want to be in a partnership with them on the assumption that we're all working toward the same goal, which is securing the health, wellbeing, and security of the United States."*
>
> -Director, Executive Branch

Join the Policymaker Hub!

WWW.BALLASTRESEARCH.COM/POLICYMAKER-HUB policymakerhub@ballastresearch.com

About Ballast Research

Ballast Research provides feedback from policymakers directly to government relations professionals, helping advocates (1) make better use of policymakers' time and (2) provide resources and materials most useful to those in government.



CAPITOL HILL

FEDERAL AGENCIES

THE WHITE HOUSE

POLICY EXPERTS

TRADE GROUPS

INTEREST GROUPS

PROFESSIONAL SOCIETIES

COMPANIES

Our Clients

Our Promise

***Confidentiality:** All participation in our research is confidential and not for attribution.*

> *"**This deep-dive, customized research is invaluable for understanding what policymakers think of us and need from us.** The insights are another important tool we use to inform our thinking on how to engage, and the data illuminates where we can do better."*
>
> -Head of US Communications, Fortune 10 Company

BALLAST

RESEARCH

Credits

Principal Author
Delia Mayor

Senior Content and Research Strategist
Allison Turnipseed

Research and Digital Engagement Manager
Sarah Devermann

Director of Qualitative Research
Matthew McCarthy

Director of Quantitative Research
Mackai Tapleshay

Chief Communications and Marketing Officer
Jamie Smith

Chief Research Officer
Michael Griffin

President
Michael Gottlieb

A Note on Use of These Materials

This document has been prepared by, and comprises valuable proprietary information belonging to Ballast Research. It is intended for educational purposes only.

Legal Caveat

Ballast Research has worked to ensure the accuracy of the information it provides in this report. This report relies upon data obtained from many sources, however, and Ballast Research is not able to guarantee the accuracy of the information or analysis contained in these materials. Furthermore, Ballast Research is not engaged in rendering legal, accounting, or any other professional services. Ballast Research specifically disclaims liability for any damages, claims or losses that may arise from a) any errors or omissions in these materials, whether caused by Ballast Research or its sources, or b) reliance upon any recommendation made by Ballast Research.

Citations

1. Peñaloza, Marisa. "Cybersecurity Attack Shuts Down A Top U.S. Gasoline Pipeline." NPR. NPR, May 8, 2021. https://www.npr.org/2021/05/08/995040240/cybersecurity-attack-shuts-downa-top-u-s-gasoline-pipeline
2. Miller, Maggie. "Lawmakers Blame SolarWinds Hack on 'Collective Failure' to Prioritize Cybersecurity." The Hill, February 26, 2021. https://thehill.com/policy/cybersecurity/540656-lawmakers-blame-solarwinds-on-collective-failure-to-prioritize
3. Hoffman, Samantha. China's Tech-Enhanced Authoritarianism Testimony before the House Permanent Select Committee on Intelligence Hearing on "China's Digital Authoritarianism: Surveillance, Influence, and Political Control" May 16, 2019. https://docs.house.gov/meetings/IG/IG00/20190516/109462/HHRG-116-IG00-Wstate-HoffmanS-20190516.pdf
4. Limbago, Andrea Little. "Digital Authoritarianism, Data Protection, and the Battle over Information Control." USENIX, January 30, 2019. https://www.usenix.org/conference/enigma2019/presentation/limbago
5. Wheeler, Tom, and David Simpson. "Why 5G Requires New Approaches to Cybersecurity." Brookings, October 25, 2019. https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

BALLAST
RESEARCH