A Penta White Paper

Penta Policy Insiders

Cybersecurity in a Digitizing World

What Policymakers Are Saying

policyinsiders.pentagroup.co

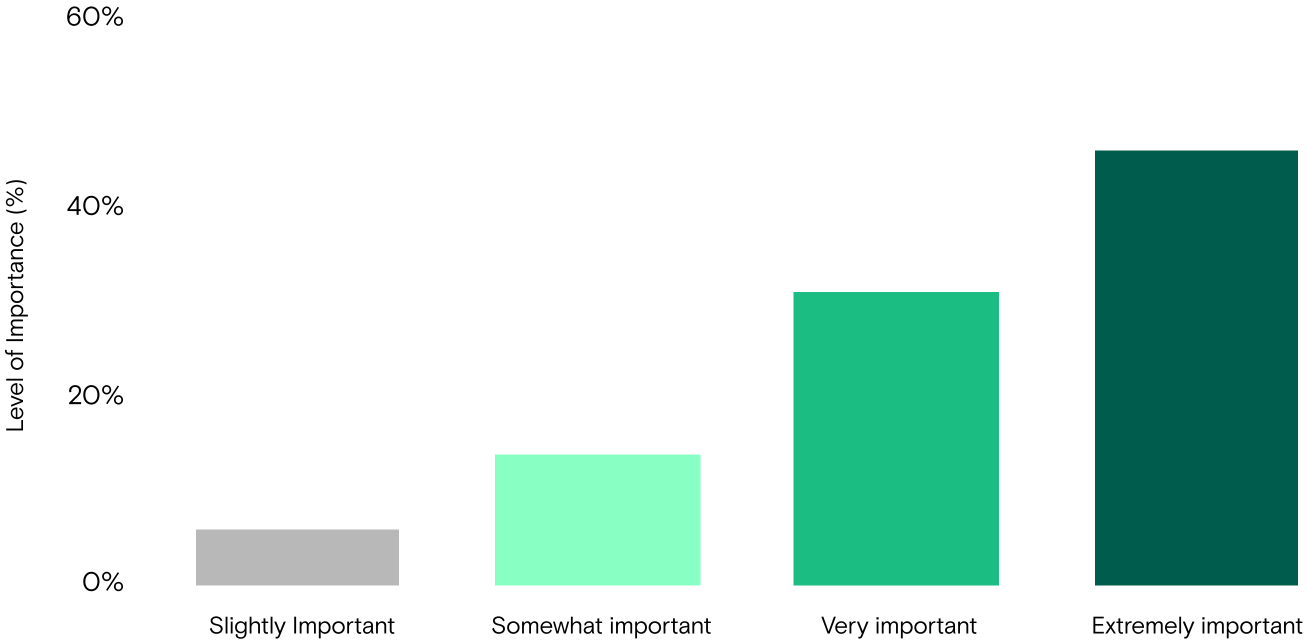
Introduction

The reliance on the internet in today's fast-paced and technology-driven society highlights both the benefits and downsides that such dependency creates. This is particularly evident when it comes to cybersecurity and data privacy, where conversations about user safety have been at the forefront of discussions among users and regulators alike. Cybersecurity, which refers to the set of actions and protocols applied to make the digital space secure, has been a focal point of policymaking in recent years. With Americans today increasingly vulnerable to cybersecurity threats, which make their personal information susceptible to attacks by bad actors, the goals of cybersecurity policies to improve elements of the digital space like data privacy and network security are more relevant than ever.[1] In fact, a whopping 77 percent of policy leaders have said that cybersecurity policy issues are either very or extremely important.

Democrat and Republican policymakers' concerns with cybersecurity come at a time when their constituents are increasingly worried about their private data. In fact, over 70 percent of consumers in the United States say they think their data is less secure than it was five years ago, and only six percent believe their data is more secure today than it was in the past.[2] With the general public's interest in ensuring the security of their data at an all-time high, we detail here policymaker perspectives on the most important aspects of cybersecurity when it comes to data privacy and regulation.

Policymaker perceptions on cybersecurity

Policymakers' views on importance of cybersecurity policy issues



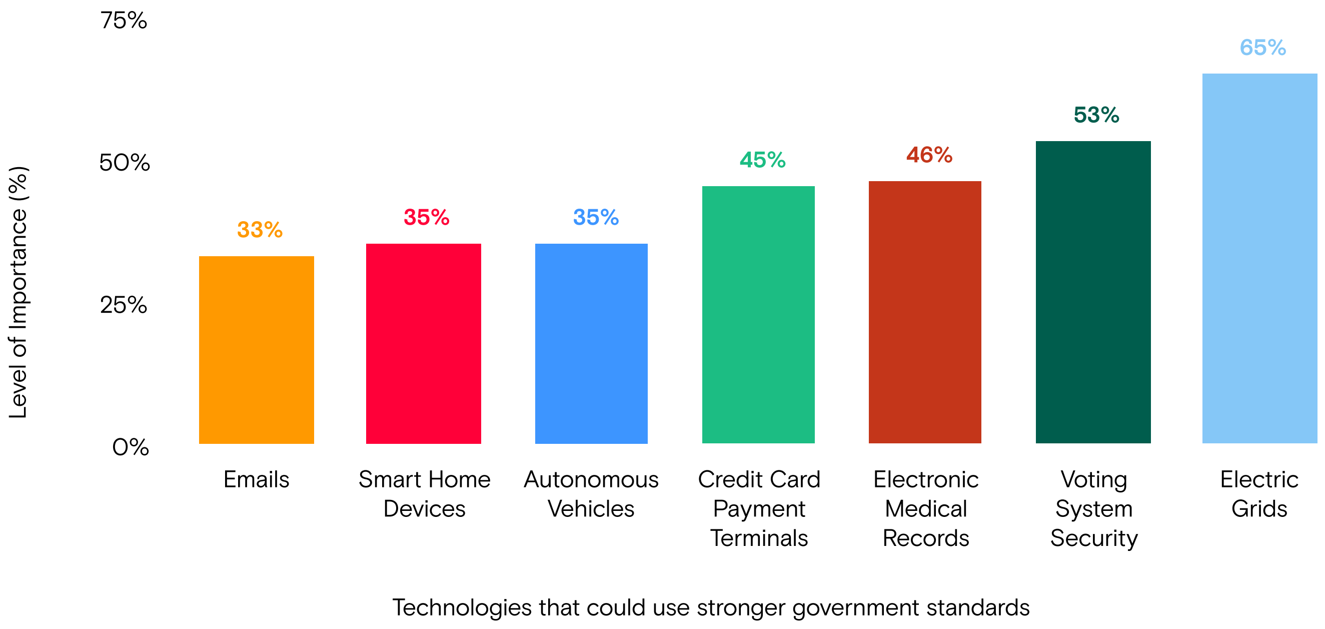
Policymakers' view on level of importance of cybersecurity policy issues

Cybersecurity and data privacy go hand-in-hand

Cybersecurity encompasses and includes multiple facets, one of which is data privacy. Data privacy broadly encompasses the industry standards, regulations, and business practices used in the handling of personal data. It refers to the protection of information ranging from data collected through fitness tracker apps to online retailers.

Many policymakers say stronger government standards to prevent cyberattacks are necessary

Areas in which policymakers say stronger government standards to prevent cyberattacks are necessary



Both Democrat and Republican policymakers agree that stronger government standards are necessary to prevent cyberattacks. Policymakers especially highlight **electric grids** and **voting systems** as areas in which policy leaders want to see more robust government intervention to ensure cybersecurity.

What are policymakers saying?

I think, though, that we should not let the government off the hook. And **I think particularly the government is responsible for consumers and their data.** And every time there's an OPM hack and government official info gets leaked like there was several years ago onward, it is dismay because it says the government can't protect you and your data."

Senior Policy Advisor, Executive Branch, D

Privacy policies are written in such a way that gives [private sector companies] the maximum amount of leeway to collect as much information as possible while availing themselves of any legal recourse that the government might have available when they get caught.

Senior Policy Advisor, U.S. House of Representatives, R

[Private sector companies] come up to the Hill and they'll say the same thing, **'Regulate us. We would love to do the right thing, just regulate us.' But it's all a little bit disingenuous because one, they have the ability to do the right thing, so to speak, without Congress telling them what to do.** And beyond that, even if they did want—they're saying they want Congress to level the playing field and pass comprehensive privacy legislation.

Chief of Staff, U.S. House of Representatives, R

I think data privacy remains the top one. Who has my data, and what are they doing with it, and can they keep it safe? A retail transaction is different than many other transactions. The people know your home address, your credit card, where you live... **All that data matters to people, and they want to make sure it's secure and safe, but they don't want to give up the convenience of purchasing it online. So it's kind of a catch-22."**

Chief of Staff, Executive Branch, R

For us **the thing that people care about the most, right, is financial security and data breaches that result in identity theft or some kind of real-world impact on customers.**

Chief of Staff, U.S. Senate, Democrat

> One of the biggest challenges we have working with the federal government on cybersecurity issues is **they're not as nimble and they can't move as quickly as some companies and AO would recommend that they do.**
>
> **Private, Partner, Political Affiliation Not Disclosed**

> Data protection is [a] huge [cybersecurity priority] because one, it's [private sector companies'] value, as I mentioned, but two, **it's the one thing that is a weak point that if their data gets compromised, then the trust in their product and their brand takes a massive hit.**
>
> **Former Chief of Staff, U.S. Congress, R**

Conclusion

Although many policymakers we spoke to agree that strengthening government standards could be the solution to improved data security, policy leaders have varying opinions on whose responsibility it is to ensure consumer data is safe. Some policymakers say it is the federal government's job to enforce regulation - and despite some calls for updated regulation on the national level - bipartisan efforts to pass a comprehensive data privacy bill in 2022 were unsuccessful, prompting some state lawmakers to propose and pass their own laws.[3, 4] As new technologies and risks emerge, data privacy and cybersecurity are likely to continue to be hot-button topics for policy and technology leaders alike on the federal level.

About Penta Policy Insiders

Penta Policy Insiders provides direct feedback from policymakers to government relations professionals, improving advocates' ability to understand, validate, and improve the efficiency and effectiveness of their engagement.

Credits

Content Associate
Maddie Markenson

Senior Content Associate
Kinda Ahmed

Associate Director, Government Insights & Research Products
Natalie Bahmanyar

Director, Research
Sehare Hemani

Associate Director, Quantitative Research
Mackai Tapleshay

Chief Research Officer
Michael Griffin

President
Michael Gottlieb

Citations

1. ttps://www.parkersoftware.com/blog/what-is-a-bad-actor-in-cybersecurity/
2. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/
3. https://www.politico.com/news/2023/02/22/statehouses-privacy-law-cybersecurity-00083775
4. https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy

A Note on Use of These Materials

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

Legal Caveat

Penta 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 Penta is not able to guarantee the accuracy of the information or analysis contained in these materials. Furthermore, Penta is not engaged in rendering legal, accounting, or any other professional services. Penta specifically disclaims liability for any damages, claims or losses that may arise from a) any errors or omissions in these materials, whether caused by Penta or its sources, or b) reliance upon any recommendation made by Penta.

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