In the face of relentless security threats, how can government preserve faith in its ability to protect citizen data?

A recent Accenture survey of more than 6,000 citizens across the United States, France, Germany, Australia, Singapore and the United Kingdom found that almost two thirds (62 percent) of respondents are less confident today in their government’s ability to defend their personal information against a security breach or a cyberattack than they were a year ago. Meanwhile, only 40% of survey respondents are confident that law enforcement agencies can protect them against cybercrime.

This decline in public trust over the last year may be due, in part, to several high-profile cyber and malware attacks in 2017, including WannaCry and Petya. More than half (58%) of respondents said these events had a direct impact on their confidence in government’s ability to protect their data. Citizens aren’t alone in their concerns about cybercrime and cyberattacks. A separate survey by Accenture and the Ponemon Institute revealed that businesses experienced an average of 130 successful cyber breaches in 2017, a figure that continues to grow year-over-year.

In today’s rapidly-evolving security landscape, government agencies – both in the United States and abroad – must find ways to better protect data and increase citizen confidence in their ability to do so.

The question is, how?

Inter-agency and cross-industry collaboration is vital to restoring citizen confidence in government’s ability to protect their personal data. Our research showed that 4 in 5 citizens support public-private sector partnerships to enhance innovation and security. This is not a surprise, given that 60% of respondents believe the private sector is more innovative than government. Government should also work with stakeholders in academia, non-profit organizations and technology companies to drive awareness and deliver new and innovative solutions that can prevent and fight digital threats.

While some government agencies are just beginning to explore opportunities for cross-sector collaboration, others are already working with businesses to create safer and more citizen-centric services and to better manage data security threats and challenges. Recently the White House Council of Economic Advisers called on public and commercial sectors to advance collaboration to address cybersecurity
risks and to reduce the impact of cybercrime on the US economy. The agency said the U.S. economy lost approximately $57 billion in 2016 due to cyber threat actors.

Despite lingering concerns about data security, citizens recognize the importance of data sharing across government agencies. Two-thirds of survey respondents believe national borders are safer when border and security agencies share information, and almost half (46%) support having multiple agencies use their data to deliver more integrated, personalized services.

**Accenture is currently working with the World Economic Forum and the Canadian Government on a Digital Traveler program**

Citizens also appreciate the role technology can play in enhancing public safety. Almost two-thirds (63%) want their local law enforcement agency to make greater use of analytics to predict crime, and a similar number think national borders would be more secure if government invested in new technologies. Accenture is currently working with the World Economic Forum and the Canadian Government on a Digital Traveler program, which will leverage blockchain to enable faster and more secure passage for pre-registered travelers arriving in Canada. Customs agencies are also using blockchain to help reduce fraud and better manage the movement of and payment for goods across borders.

**Conclusion**

The rapid pace of technology change means that new threats are emerging every day. Fortunately, government agencies don’t have to face these challenges alone. By leveraging new technologies and forming innovative partnerships, public sector organizations will not only be better prepared to anticipate and respond to evolving threats – both online and in the real world, they’ll also inspire greater confidence in their ability to protect citizens and their data.

* This article was published by [www.nextgov.com](http://www.nextgov.com) on April 6th 2018