Mitigating Election Security Risks Rely on System Resiliency, Auditability

New report finds identity theft, financial and election security among top consumer concerns.

Amanda Ziadeh

Wed, 10/24/2018 - 16:59

DHS Undersecretary Christopher Krebs at GovernmentCIO Media's CXO Tech Forum: The State of Cyber Oct. 4. (Geoff Livingston/GovernmentCIO Media)

A continuous increase of data breaches, the 2016 election interferences and financial security concerns are causing a riff in the public's cybersecurity trust in government and industry, and could impact whether people show to vote.

That's according to global IT company Unisys' annual security index, a look at global and national security concerns. The index is a calculated score out of 300 that measures consumer concerns over time across eight areas of security in four

categories: national security, financial security, internet security and personal security.

This year’s index is 173, same as last year, but 32 percent higher than 10 years ago, according to the report. And the highest security concerns people have are around identity theft and bankcard fraud.

In fact, identity theft was one of the top eight security threats measured, coming before national security (including terrorism), disasters and epidemics, financial obligations, bankcard fraud, viruses and hacking, online transactions and personal safety.

The report found that 68 percent of respondents are seriously concerned, meaning extremely or very, about identity theft. Bankcard fraud followed with 66 percent seriously concerned, then disasters and epidemics and national security.

Perhaps more relevant with the midterm elections approaching is the report’s findings that average American respondents are concerned about election security. Eighty-six percent of U.S. consumers have some level of concern that their election voting system can be tampered with by outside actors, according to the report.

But these results regarding election security don’t necessarily surprise Homeland Security Department Undersecretary Christopher Krebs.

“It’s relatively new . . . election security just kind of hit the public awareness in the last two years,” Krebs said at the Oct. 24 Unisys Global Security Index survey panel in Washington, D.C.

He pointed to the 2016 election interferences as the moment the public realized cybersecurity could destabilize the government and democracy, rather than just risking intellectual property.

“So, we need to better engage on kind of a psycho-social confidence side of cybersecurity,” Krebs said.

The increase in internet security concerns and hacking shouldn’t come to a surprise either after Russian interference in the 2016 elections. The report found that viruses and hacking has increased from fourth to third place in global security concerns, most likely caused by the increase of data breaches of personal and financial data. And these data breaches are still happening, potentially causing this high concern

about identity theft or credit card fraud over concerns about terrorism.

Closing the Citizen-Government Trust Gap

The report suggested that viruses and hacking are creating a trust gap that public and private industry need to address. These attacks are the third highest global security concern, according to Unisys' index, and consumers are constantly hearing about breaches in the news that impact millions of people.

"They are starting to question aspects of their interactions with businesses and governments in ways they had not done previously," the report said, and the news of all this hacking is causing citizens of democracies to lose confidence in the election systems, especially in the U.S..

Krebs said one of the unique and valuable elements of the Unisys report is its emphasis on consumer confidence.

"The federal government in and of itself does not necessarily have an oriented mechanism to address the confidence element of cybersecurity," Krebs said, and DHS' National Protection and Programs Directorate more so focuses on hard infrastructure challenges and technical issues.

But this lack of confidence has its implications. Unisys found that nearly one in five U.S. consumers said they will not vote or are unlikely to vote in the 2018 midterm elections, simply due to concerns around election tampering.

What's the Solution?

It's paper ballots and audible systems, according to Krebs.

"Election security is about resilience in the system, and auditability, and understanding where your last good point is so you can validate the results, and to that end, audibility being a core tenant of IT security," he said. So, how do we get there? "It's paper ballots paper ballots paper ballots, audits audits audits."

At the end of the day, the systems that support election systems are IT systems, and by the nature of IT systems, they have vulnerabilities. This feeds into resiliency, because there's the management system and there's the actual voting tabulation system, and the real risk in the system at a global and national scale in terms of

being able to vote is the threat of a technical manipulation of the tabulation system.

“Going to the process of voting, it’s all about resilience. If something happens, do you have the ability to check your work? Check your map, audit the system, look for those paper ballots?” Krebs questioned.

And though paper ballots aren't foolproof, it’s another measure to fall back on. Along with physical security controls, having hard, tangible fall backs and audibility provide confidence in the system and resilience in the process to identify where something went wrong.

See Something, Say Something

Election security also relies on federal, state and local governments working together and sharing information, something DHS has been working to improve and making progress with.

Krebs said two years ago, there wasn’t a strong relationship between state and federal government in election security, which resulted in a lack of an over-the-top understanding of the profiles of election systems.

Now, thanks to efforts like the Election Infrastructure Information Sharing and Analysis Center, that relationship is there, and DHS is working with all 50 states in some way shape or form. And it’s not all states are doing; they have in-house capabilities, contract with third party vendors, and so on.

But the EI-ISAC expands DHS’ broader mission working encouraging a “see something, say something” approach.

“If the state or local election official just sees anything out of the ordinary, let us know, and as long as we’ve got the rest of the election community doing the same, funneling it, we’re able to identify trends and anomalies across a larger set of networks a lot quicker than we were two years ago,” Krebs said.

View printer friendly version
Department of Homeland Security
Christopher Krebs
election security
Federal Cybersecurity

election
CXO Tech Forum State Cyber