



THE MISSING AGENDA

THE IMPORTANCE OF CYBER SECURITY TO U.S. VOTERS

This election season voters have heard promises to make the U.S. great again and how we're stronger together. But they have yet to hear an adequate answer from either Hillary Clinton or Donald Trump on how they would handle cyber security as president. This is according to the results of a Cybereason survey that looked at how information security factors into November's election.



While perennial issues like economic policies, education and health care still matter to voters, they also care deeply about how the next commander-in-chief will protect the nation from cyber attacks, judging by our survey, which polled 515 registered U.S. voters in 47 states.

CYBER ATTACKS POSE A GREATER THREAT THAN ISIS

In matters of national security, 70 percent of respondents said that cyber attacks were more threatening than ISIS, climate change and nuclear weapons.

And cyber security isn't just a concern in the context of national security. It's one of the most important issues to the country's future, according to 53 percent of the voters we polled.

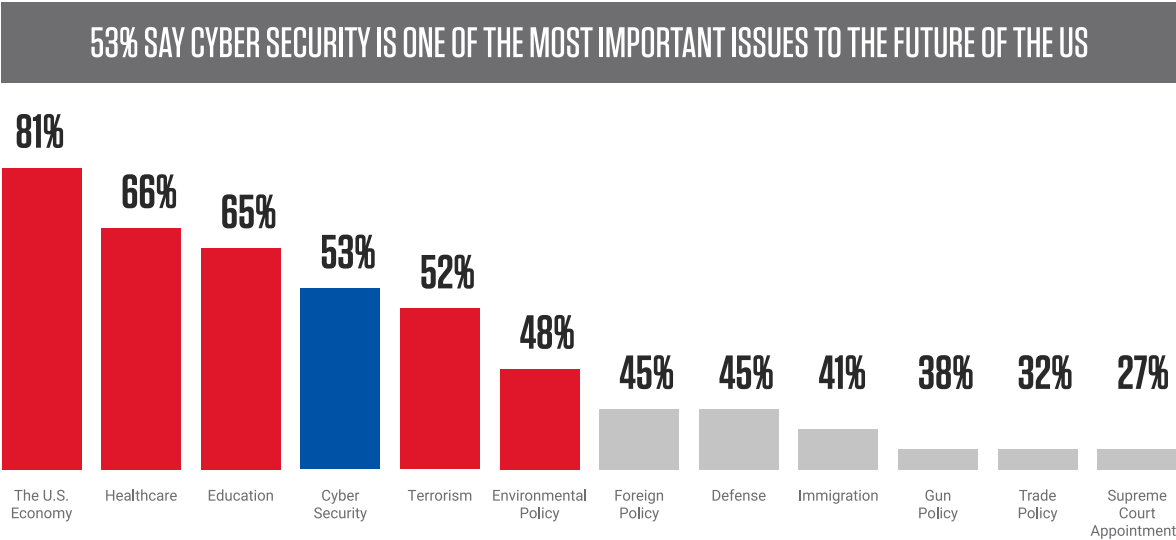


70%
of respondents
selected cyber
attacks as a
big threat to
national
security.

More threatening than
ISIS, climate change,
and nuclear weapons

CYBER SECURITY RANKS HIGH ON VOTERS' AGENDA

Out of the 12 issues listed, respondents ranked cyber security fourth. Only the economy (81 percent), health care (66 percent) and education (65 percent) were deemed more important. Cyber security beat out terrorism, environmental policy, foreign policy, immigration, gun policy, trade policy and Supreme Court appointments as top election issues.



To understand why information security is such an important issue to voters, look at the spate of cyber attacks and data breaches that have dominated the headlines in recent years. Some of the more notable ones include the 2013 Target breach (which is considered the incident that helped the public fully understand how information security affects them), the 2014 JP Morgan Chase and Sony hacks, the Office of Personnel Management and Anthem breaches in 2015 and the attacks against the Democratic National Committee and Yahoo in 2016.

OLD AND NEW THREATS DRIVE CONCERN


As the scope, scale and frequency of attacks increase, these incidents are impacting more people. Our survey found that **35 percent of respondents have been the victims of cyber attacks**, such as having their password or identity stolen. The voters surveyed showed a savviness about the many threats that attackers are using. Most of the voters are concerned about **malware (77 percent), phishing scams (55 percent), ransomware (53 percent), denial-of-service attacks (53 percent) and malvertising (30 percent)**.

Given this information, perhaps it's unsurprising to learn that 77 percent of the people we polled are more concerned about cyber security than they were during the last presidential election. Additionally, the cyber risk against the U.S. is greater now than it was during the 2012 election, according to 81 percent of respondents.

And, of course, since this summer the U.S. government has accused Russia or groups linked to the Russian government of attempting to influence the U.S. election by hacking the email accounts of political organizations and campaign advisers. Maybe this is why **65 percent of the people who were surveyed said that they are concerned about a major cyber attack being launched against the U.S.**

Despite fears about the U.S. suffering a major cyber attack, respondents had a more sanguine view about the prospects of an attack being used to sway the presidential election, with 37 percent saying that could happen. When asked if such an attack was likely to happen, the responses were even more positive: only 15 percent said such a scenario is likely.

Given how concerned voters are about information security issues, you'd think the Democratic and Republican presidential nominees would be more attuned to this topic. But our survey suggests otherwise. Neither Clinton or Trump have shared enough details on their respective plans to protect against attacks, said 70 percent of the respondents.



Given how concerned voters are about information security issues, you would think the Democratic and Republican presidential nominees would be more attune to this topic. But our survey suggests otherwise. Neither Clinton nor Trump have shared enough details on their respective plans to protect against attacks, said 70 percent of the respondents.

51%

DON'T THINK EITHER CANDIDATE UNDERSTANDS THE COMPLEXITY OF CYBER SECURITY

Perhaps they watched the second presidential debate when the sole question on cyber security yielded the theory that obese people hacking from their beds are responsible for attacks and the predictable answer that cyber security is a huge issue. Given that these answers left much more to be desired.

55%

LACK OF CYBER SECURITY EXPERIENCE

A lack of direct experience (55 percent) in dealing with cyber security was another factor voters listed as the reason behind their lack of confidence in Clinton and Trump's abilities to understand information security.

And don't expect either candidate's cyber-security advisers to impress the voters, 50 percent of whom said Clinton and Trump have picked the wrong people.

76%

TECH TAKE THE WHEEL

Voters believe that major technology companies like Google and Facebook have a responsibility to help protect the U.S. from cyber attacks, said 76 percent of respondents. There's the perception that companies have made more progress than the public sector in preventing attacks, said 71 percent of respondents.

VOTERS CARE ABOUT CYBER SECURITY, CONTRARY TO THE INSIGNIFICANT AMOUNT OF ATTENTION THE TOPIC HAS RECEIVED DURING THIS PRESIDENTIAL CAMPAIGN.

Major data breaches at businesses from every industry as well as government organizations have proven that no one is immune to an attack. Voters seem to realize this more than the people they are choosing between to run the country.

With the final presidential debate scheduled for tonight, Clinton and Trump should find a way to offer more details on their respective information security plans.

Earning a person's vote involves more than pledges to lower taxes or speeches on clean energy: how the candidates will handle "the cyber" greatly influences who voters pick to occupy the White House.



Founded by members of the Israeli intelligence agency's elite cyber security Unit 8200, Cybereason mirrors the founders' expertise in managing some of the world's most complex hacking operations. Cybereason developed the world's only military-grade, real-time detection and response platform and has a proven track record of protecting Fortune 1,000 enterprises globally. The company has received many awards and accolades since its founding.

Cybereason is privately held and headquartered in Boston with offices in Tel Aviv and Tokyo.

