VIEWPOINT

Send letters to the Pittsburgh Business Times
45 S. 23rd St., Suite 200 Pittsburgh, PA 15203
pittsburgh@bizjournals.com

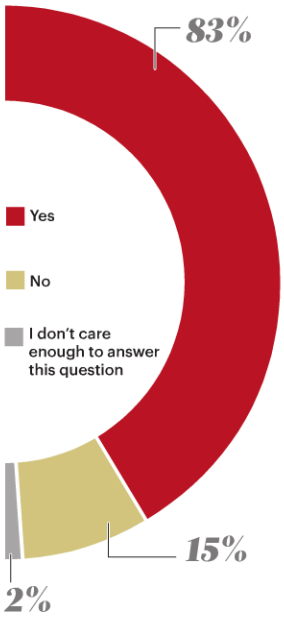
PULSE SURVEY

WE ASKED

SERIOUSLY, DOES VOTING REALLY MATTER?

YOU ANSWERED

1,530 responses



COMMENTS

The simple answer to a very simple question is yes, it does matter. It matters very much to have the right to vote and then to actually vote.

I once was a big believer in the vote – and I used to volunteer to put out the vote. But now, in my late 40s, I don't feel voting for someone who is running for office matters — it's all about who has the biggest budget for ads and who slams their opponent. No, I don't believe that voting for a person makes a difference anymore because I don't believe candidates hold true to what they campaign on. However, voting on props and issues — yes, I do.

THIS WEEK'S QUESTION

Who should be responsible for helping veterans transition back into civilian jobs? **Vote here:** bizj.us/15284v

► WHAT DO YOU THINK

We want to hear your opinion on the issues you read about in the Pittsburgh Business Times. Submit letters to the editor to PittsburghBusinessTimes.com or call Managing Editor Jennifer Curry at 412-208-3820 with questions.

VOICES OF PITT

The need for vigilance with cybersecurity

The cloud is hanging over us.

Five years ago, it might have been sufficient for businesses to manage cybersecurity by banning employee-supplied devices, restricting information systems to "fixed location" devices (like desktops) and encrypting mobile devices that were absolute business needs. These types of aggressive security measures, however, simply aren't feasible in today's business environment.

As younger employees raised in the Information Age increasingly overtake the majority of professional positions and social networking replaces the traditional telephone as the primary means of personal communication, employees expect to be able to use modern technologies, like cloud storage, to get work done. Not to mention there is increasing pressure on marketing, communications and sales representatives to utilize social media, and pressure on accounting and finance divisions to provide electronic billing and other e-commerce functions. Plus there's pressure on operations professionals to provide informatics on logistics, inventory and other data for predictive purposes. These pressures collectively mount and, as a business

David Thaw is assistant professor of law and information sciences at the University of Pittsburgh.

leader, you're eventually forced to embrace technology.

What's the result? Your business is a part of the world's network, regardless of whether you would prefer for it to be offline. What businesses often fail to realize is now they're not just targets, but they're also tools for attack. Certainly an HVAC vendor that fixes air conditioning units isn't at the forefront of the IT industry and isn't expected to have expertise in cybersecurity. Such vendors don't have much in the way of sensitive data, and what they do have probably isn't something organized crime has much interest in. But these vendors are obvious tools for attackers.

In the 2013 Target data breach, the attackers got in via one of Target's vendors. And this is not the only way a company can become a tool. If you have a network of tens of thousands of devices – and an attacker can penetrate that network and distribute malicious software to those devices – that attacker can use your network to launch an attack. Throughout both my academic career and in the private sector, I have been deeply invested in an ongoing push to secure information systems against such technology-based crimes.

So, how should business leaders respond? They should engage and invest in risk mitigation – informed by the analyses of qualified professionals familiar with the private sector – to determine the proper level of information security for their systems. Step one is conducting a risk assessment, and step two is developing a risk mitigation security plan based on that assessment. Instead of focusing on building impenetrable systems like in years past, they should commit to systematically reducing the risks of data insecurity. Security plans should be updated regularly using ongoing risk assessments. Being vigilant will help to chase rainy days away from your company – and your company's partners, too.