LAMORINDA WEEKLY
Independent, locally owned and operated!
www.lamorindaweekly.com 925-377-0977

Published May 2nd, 2018

Understanding broader perspectives of personal cyber security

By Lou Fancher

The safest path to cyber security is paved with knowledge and fortified by balanced perspective, according to experts in the field. It's a mindset well-suited to that of the East Bay chapter of the World Affairs Council, whose mission is to provide communities with neutral forums and expert speakers on global topics that include human rights, health, technology, government and more.

On April 25 at the Lafayette Library and Learning Center, the 60-minute program presented by EBWAC addressed cyber security. Led by Benjamin Bartlett, a Ph.D. candidate in the Charles and Louise Travers Department of Political Science at the University of California at Berkeley, the presentation clarified cultural and political similarities and differences within governments and citizens in the United States, Europe and Japan.

Bartlett offered technical expertise from work as a computer programmer prior to his current concentration: conducting field research on security policy in Japan. Stating his intention-to leave people with awareness and knowledge to independently discuss the topic after the forum-Bartlett said understanding the differences allows people in the U.S. to make informed choices about protecting their cyber security.

"We're not going to get a better deal with things like personal security unless people actually get out and vote for it," he said. Civic engagement expressed through political activism, he suggested, therefore requires deep understanding of how countries and governments approach cyber security.

"In the United States, cyber space is viewed by government a domain like air or water where we have to duke it out with other actors," he said. This framing of cyber security as a national defense issue means countries like North Korea that may have less military firepower - missiles, bombs, ships, airplanes - may build vast, cheaper-to-produce software and malware and be highly threatening. The U.S. perspective results in laws and policies that protect national security over personal privacy. Homeland security, government intelligence gathering and shielding the U.S. during conflicts with other countries vastly outweigh protecting citizens and businesses from hackers and malware. "The NSA (National Security Agency) is less interested in personal encryption programs or protections because they want to be able to access that data too," said Bartlett.

In Japan, threats to cyber security are perceived as coming from outside hackers and criminals. The government believes citizens need encouragement to protect themselves from direct attacks. The dominant viewpoint results in government-sponsored ads, like one comic-book style scenario that has a young man about to kiss a woman declare, pseudo-romantically, "Such a weak password, doesn't suit you." Classes in schools teach young people how to create safe passwords, use patches and update protection software or have operating systems swept clean of malware.

The European Union's 28 member states emphasize personal privacy as does Japan, but highlight control. The primary concern for Europeans is ownership of personal data. "They worry about Facebook and Google, not just because of hackers, but because of the ways the data can be used by the companies," Bartlett said.

In a case involving Google, a 12-year-old newspaper report about a company in Spain that had been in financial trouble was picked up by Google and put online. "Suddenly, the archival information meant people viewing the owner's profile started to react to his at one time having been in financial trouble," said Bartlett. "Google's argument was that it was public information. Europeans didn't agree and said it fell under their 'right to be forgotten' rules. They said it was causing the man a lot of damage." The government now has stronger laws that guarantee protection, including rules that any information people delete from their data files cannot be stored elsewhere by internet providers.

Questions from the audience displayed familiarity with cyber security basics. Jumping well past safe passwords, hackers and phishing tactics, people asked about Russia's involvement in the 2016 election, China's highly censored internet and Facebook's crisis and coverup involving data-science firm Cambridge Analytica obtaining 50 million Facebook users' data. Bartlett said there is no evidence that Russia altered U.S. citizens' votes, but there is clear indication that voters were targeted with massive misinformation.

Asked if the government is likely to take specific action to prevent future problems, he said, "There's a lot of talking about it, but I haven't seen any action. The problem with the U.S. is that we can't do it without cracking down on countries and to a certain extent, on our free speech rights. You could not pick a better country to do this to, in some ways."

On China, he said the government that controls a tight, interlocked internet ecosystem is primarily concerned with their citizens' online activities, not that of outside actors. Facebook, Bartlett suggested, has no incentive to make changes as long as they are making money. No one was thinking about security when the internet and social media platforms were created. "They were just inventing something cool," he said.

A clear question - a subject ripe for more discussion - lingered as people left the presentation. How much freedom are Americans willing to sacrifice or turn over to the government to gain greater cyber security?

To learn about the WAC and future events, visit http://www.worldaffairs.org/index.php

Reach the reporter at: info@lamorindaweekly.com

back

©

Copyright Lamorinda Weekly, Moraga CA