Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

cybersecurity has already begun, and it could become a matter of serious concern quickly. (Think China Syndrome, only with cyber in the place of cold-war, secret nuclear ...

Jan. 16, 2019

With the record-setting phase of the federal shutdown now underway, the war over how best to protect the US-Mexico border is seriously impacting our country's

cybersecurity, and, with that, imperiling our nation. This is not about partisan

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

suffering in the same way as wholly shuttered agencies, and you are right. But relativism in cyber-related tasks is dangerous. The reduction in work hours across the board could well create vulnerabilities. Software updates, security patches, memos regarding phishing campaigns — all of that will take a hit with diminished recourses, and "that" is a major part of keeping the barbarians beyond the gates.

At issue here is something akin to a riddle: Who will monitor the monitors if the monitors aren't being monitored? What if they aren't working? Effective cybersecurity is maintained by an ecosystem of practices and measures. Unfortunately, we may not find out the answer until long after the shutdown has ended — when news breaks that there was a serious breach at one of the federal agencies as a result of the reduced staffing of that ecosystem.

The roughly 800,000 federal workers currently on furlough include:

- 45 percent of the staff from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, which is tasked with defending critical infrastructure from cyber and physical threats;
- 80 percent of the National Protection and Programs Directorate, which oversees the Office of Cyber and Infrastructure Analysis and the Office of Cybersecurity and Communications;
- 85 percent of the National Institute of Standards and Technology, which produces the Cybersecurity Framework of private and public sector security standards.

The monitors need backup, but with skeleton crews in place, it is quite possible those tasked with making sure breaches haven't occurred are unable to do their jobs, and their backup —well, there is none.

As Govtech.com noted, "Departments and agencies affected by the shutdown include the departments of State, Homeland Security, Agriculture, Commerce and Housing

and Urban Development, as well as the Environmental Protection Agency, the

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

determine what the United States considers to be critical systems. They will be looking at activity in the cybersecurity ecosystem, and how it has changed.

The federal government uses a small army of contractors to monitor federal agencies. These non-government cybersecurity contractors have to get paid to work. And they are crucial. These are often the parties responsible for testing the system, looking for vulnerabilities and signs of incursion, running penetration tests, making sure the latest security patches have been installed as well as many other tasks that are mission critical in the effort to protect the nation from attack, both from without and within our national borders.

Right now, we have no idea what's being done, and what's not getting done, and that matters.

Even with the most hands-on approach to our national cybersecurity, we've been hacked — think OPM, USPS, SEC, etc. Four of the ten biggest government breaches were federal. And those were when the government was fully staffed.

This situation is untenable and endangers our democracy from threats abroad in ways that show the so-called "emergency" on the Rio Grande for what it is: a dangerous political gambit that could cause a very real emergency.

========

Adam K. Levin is a consumer advocate with more than 30 years of experience and is a nationally recognized expert on cybersecurity, privacy, identity theft, fraud, and personal finance. A former Director of the New Jersey Division of Consumer Affairs, Mr. Levin is Chairman and founder of CyberScout and co-founder of Credit.com. Adam Levin is the author of Amazon Best Selling Book Swiped: How to Protect Yourself in a World Full of Scammers, Phishers and Identity Thieves.

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us