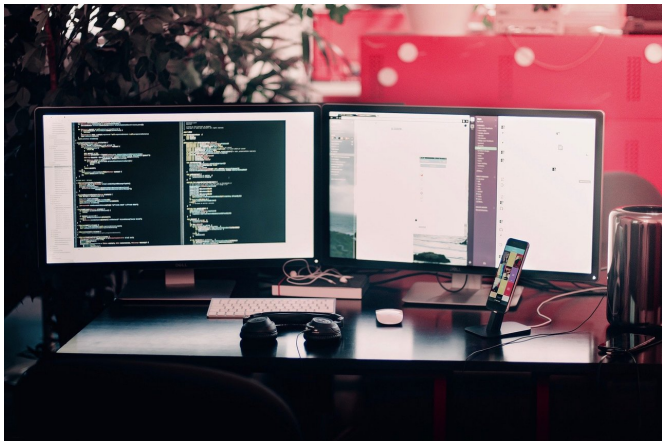
With many federal employees working from home, cybersecurity experts look to beef up defenses

31 August 2020, by Brian Contreras, Los Angeles Times



Credit: CC0 Public Domain

In the age of social distancing, many employees have found their workplace shift from an office cubicle to a living room couch.

But for federal workers and IT teams who often handle sensitive data using outdated government systems and infrastructure, working from home brings new challenges—particularly as concerns are rising about cybersecurity attacks seeking to exploit the pandemic.

Lawmakers say the government should move quickly to modernize its IT infrastructure.

"The large-scale shift to telework exposed critical cybersecurity vulnerabilities underlying that outdated IT," said Rep. Gerald E. Connolly (D-Va.) during a recent House hearing on federal tech modernization. "Since the pandemic hit, ... inspectors general have reported increased risk of data security breaches, disclosures of classified information and targeted cyberattacks and fraud schemes."

Indeed, a June report from the federal Pandemic Response Accountability Committee cited concerns from the National Reconnaissance Office's inspector general about "inadvertent spills and disclosures of classified information by employees performing unclassified work at home" thanks to weak passwords and unsecured Wi-Fi routers, cellphones and social media platforms.

Inspectors general for the Peace Corps and Environmental Protection Agency raised similar concerns.

And in March, the Department of Health and Human Services was the target of a highly publicized hacking attempt, although it was unclear whether state actors or criminal hackers were responsible. Around the same time, security experts noted a rise in COVID-related phishing attempts targeting government employees.

The federal government isn't alone in reckoning with this issue. Experts predict both government and private industry will need to rethink how they protect their systems and information in light of the rise in teleworking, which could continue even after the pandemic ends.

"These changes that we're seeing on the IT side are not temporary," said Bryan Ware, assistant director for cybersecurity at the Cybersecurity and Infrastructure Security Agency. "In my view, they are permanent. It will change the way that we have to look at security. It will change the way we have to look at protecting sensitive information, not just cybersecurity, because the enterprise perimeter is now extended into a person's home."

He added, "I expect there's going to be really

transformational changes in cybersecurity in almost every facet of what we do."

Cyberthreats against both the government and private sector are only increasing.

On a global scale, Interpol has noted a shift in the targets of cybercrime from individuals and small businesses to corporations and governments. More locally, the city of Los Angeles' Information Technology Agency reports about a 25% increase in phishing emails sent to city employees.

These threats have prompted some agencies to adopt a mix of new training protocols and digital defenses to account for a more spread-out workforce.

The Department of Veterans Affairs, for instance, says it has introduced a new security platform and phishing reporting system, while also increasing staff privacy training.

And for Los Angeles city employees, certain work done on personal devices can only be accessed through a "sandboxing" platform, which cordons off the contents from the rest of the device, according to the L.A. Information Technology Agency.

Some government agencies began such changes before the pandemic.

The General Services Administration, for example, always functioned "a bit like a commercial venture," said chief information officer David Shive, because employees were spread out in different locations.

"We create a perimeter defense around our people and around our devices rather than the core central systems," he said. So while the coronavirus meant some agencies "had to change their cybersecurity posture and stance, we didn't have to really change anything."

The General Services Administration views itself as a "pilot space," trying out new things before expanding successes to the rest of the federal government, Shive said. In that regard, the agency could become a model for how the rest of the government deals with telework going forward.

"It's forcing us, in a good way, to make sure we're not only digital, but as efficiently digital as possible," he said. "That's good work, and I suspect that that will continue on long after the pandemic is over."

Not every agency reports increased cyberattacks during the pandemic.

Spokespeople for the Departments of Justice and Veterans Affairs said their agencies haven't experienced an uptick. The National Science Foundation said it has neither seen an increase in phishing attempts nor experienced any security incidents involving employees at home. The Department of Agriculture said whatever change it has seen "hasn't been unusually noteworthy."

David Nelson, chief information officer at the Nuclear Regulatory Commission, said his agency has actually seen a decrease in phishing and other attacks.

But one common thread among government agencies is that phishing email attacks frequently try to exploit fears and concerns about the pandemic.

"At the Department of Justice, COVID-related phishing attacks generally use content that advertises availability of personal protective equipment with links to malicious sites," a department spokesperson said. "In some cases, an attacker may attempt to initiate a back-and-forth email conversation with a target user regarding the challenges of COVID-19."

Another type of attack involves emails that imitate an agency's IT help desk, telling employees to log into a web portal and report their work-from-home availability, said the L.A. Information Technology Agency's chief information security officer Timothy Lee. The link in the email is, of course, fake.

Such tactics are nothing new.

"Whether it's civil unrest or a pandemic or the NCAA Final Four or the Academy Awards or anything like that, their playbook is pretty rote," the GSA's Shive said. "They just tailor it based on what the information of the day is. It just so happens that

we're going through a pandemic."

APA citation: With many federal employees working from home, cybersecurity experts look to beef up defenses (2020, August 31) retrieved 18 June 2021 from https://techxplore.com/news/2020-08-federal-employees-home-cybersecurity-experts.html