The Next Cybersecurity Pandemic: Are We Prepared?

Summary of Roundtable, hosted by ATARC in September 2022

WHITE PAPER

Cybersecurity has become a fundamental and vital component of U.S. policy. As a data-driven nation, there is obvious need for an ultra-secure government network. Recent high-profile events like *SolarWinds* and *Colonial Pipeline* remind us that the next cybersecurity disaster could be just around the corner. This is only the beginning: as threats evolve, federal agencies must keep pace.

To its credit, the U.S. Government has taken legislative actions, with presidents signing executive orders to strengthen Federal cyber defenses and Congress passing strict laws to combat cybercrimes. Initiatives like Zero Trust and other security efforts are well underway.

But is that enough? Have we reached our goals? What still remains to be accomplished? Are adequately high expectations being set for contractors to deliver applications and services that ensure the government is not left vulnerable to attack? And are they held to those expectations?

To answer these questions, ATARC hosted a roundtable on cybersecurity preparedness, lessons learned from previous incidents, and containment and prevention measures undertaken to mitigate potential future threats.

Get Ahead, Stay Ahead

U.S. Government's digital infrastructure holds a massive amount of personal information about the nation's citizens. Protecting this data is obviously of utmost priority, but not an easy task. Participants shared insights about the government's challenges in safe-guarding the public-facing digital infrastructure against hackers and being ready for the next potential security breach.

Predictably, the most frequently cited obstacles included limited budgets and lack of resources. Agencies large and small, including those considered to be high-profile targets for our adversaries, are perennially underfunded.
Frustration with getting appropriators and Congress to understand the magnitude of necessary costs and staffing was a common issue. In one participant's example, upon being requested by Congress to estimate their needs to prepare for another SolarWinds-like attack, the agency presented a calculation of $250 million needed to adopt Zero Trust architecture. The Congress approved only $130 million, of which merely $10 million was actually disbursed, significantly restricting the department's ability to take action.

Biggest Obstacles to Cyber Preparedness

Roundtable participants agreed that the biggest challenges to cybersecurity preparedness are:

- Lack of qualified applicants
- Lack of budgetary resources
- Legacy code and incompatible infrastructure
- Inefficient and cumbersome hiring processes

Many agencies have traditionally failed to keep pace with modernization. Several participants mentioned struggling with decades old code and infrastructure, often antiquated to the point of no upgrade options. IT departments must carry the extra burden of quarantining these obsolete systems from the rest of the network, which taxes the productivity of an already strained workforce.

Labor Market Challenges

Participants also pointed out the plight of recruiting and retaining talent. While it affects the entire job market, the public sector has been hit especially hard. Agencies often lose critical employees to industry, which can easily attract top talent with more lucrative benefits and compensation.

High turnover has led some agencies to prioritize and spread out their cybersecurity initiatives. Others cited frustration with training employees only to have them leave after completing the program. One participant noted planning their training around the expectation that as much as 70% of the trainees will leave in the short term.

Participants also wish to see more of "outside the box" thinking and problem solving in their workforce. This may reflect the government's inability to compete for top talent and inefficient hiring processes makes recruiting higher level skills but impossible.

A desire to modernize the hiring process and offer clear career paths for new hires emerged as a common theme throughout the roundtable. Participants that transitioned from industry highlighted the differences that appear already in the earliest stages of the hiring process. Where in the private sector, a single person oversees sorting through resumes, this first step of candidate selection can take months in the government.

There is true concern about the lack of clarity in career advancement paths. The overall candidate pool will likely have a significant number of recent graduates or applicants with relatively short resumes. In the private sector, there are ample growth opportunities to move up from junior level positions. In today's tight labor market, all successful employers must offer attractive benefits and well-defined advancement options.

Employee Turnover Crisis

According to Gartner[1], U.S. annual employee turnover for 2022 will likely jump **20% above pre-pandemic levels**

A recent study by McKinsey proves this point. The consulting firm found that 40% of all workers plan to leave their jobs within three to six months. While one might expect better compensation as a primary reason for changing jobs, flexibility and upwards movement ability are equally important for many job seekers.

Finally, OMB A-76's mandate for government entities to outsource to the private sector in situations where commercial options are readily available, was also mentioned as a barrier to recruiting new talent. This directive was last revised in 1999 and has not been updated since. Participants noted that the effects of this outdated directive have been largely negative. As agencies attempt to hire new in-house IT personnel, some found agency heads unwilling to provide funding, citing OMB A-76 as the reason.

Due to the hurdles along finding and hiring talent, it is no surprise that some agencies have started relying heavily on contractors. While convenient, contractors pose a bigger security risk because of the agency's reduced ability to control their devices and online behavior.

Participants noted that they already struggle to meet the cybersecurity demands of a now largely remote workforce. Some estimate that as much as three quarters of their agency staff are now permanently telecommuting. Contractors compound this problem and may expand an agency's attack surface in unforeseen ways.

Keeping pace with important cybersecurity mandates (whether funded or not) is essential. Experts at the roundtable recommended establishing a strong authentication perimeter before moving on to other efforts. This should provide both certainty of identity and assurance that the device used is not compromised (commonly referred to as risk-based authentication).

Vendors should be held equally accountable. Agencies that handle sensitive constituent information daily need to be equipped with secure and resilient code, applications, and services. The government must do a better job of ensuring that vendors are not opening it up to attack.

The U.S. Digital Service

Following the issue plagued Healthcare.gov rollout, the Obama Administration created the U.S. Digital Service (USDS). This organization recruits private sector experts across IT disciplines to address some of the country's most significant technical challenges. Agencies can leverage USDS to address their most pressing issues faster than via their inefficient hiring process.

While USDS-enlisted skill sets may be helpful, participants also suggested mirroring their recruitment strategies to attract top talent. The calling of being in public service and the ability to effect real change might speak louder than a large paycheck at a generic office job. Realizing this, the USDS recruitment efforts are centered around the concept of service, demonstrated progress, and the potential to make a difference.

Check out Cybersecurity themed events and Working Groups facilitated by **ATARC** to help solve pressing challenges within Federal Government with the help of emerging technologies.

[1] Gartner Newsroom, April 2022