February 2019

CYBER PERSONNEL ARE ESSENTIAL STAFF

FEDERAL RECRUITMENT & RETENTION IN POST SHUTDOWN AMERICA

Authored By:

Drew Spaniel, Lead Researcher, ICIT
Parham Eftekhari, Executive Director, ICIT

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Cyber Personnel Are Essential Staff

Federal Recruitment & Retention in Post Shutdown America

February 2019

The authors would like to thank the following ICIT Fellows for their advisement and expertise which supported the development of this paper. The views expressed in this paper are those of the authors, not that of the Fellows listed below.

- Don Maclean, ICIT Fellow & Chief Cyber Security Technologist, DLT
- Robert Wood, ICIT Fellow & Chief Security Officer, Simon Data

Contents

Introduction

One of the most underreported yet greatest national security impacts resulting from the 2018-2019 government shutdown will be the unmeasurable loss of an entire generation of cybersecurity professionals who may exit the federal workforce or not consider it a viable career path in the first place. S&P Global Rating estimated a loss of $6 billion in direct costs as a result of the shutdown. The Congressional Budget Office estimated that the 35-day partial shutdown cost $11 billion [1]. Neither of the estimates is adequate when factoring in costs associated with the long-term loss of cyber talent or the tangible and intangible costs associated with cyber adversaries who may have compromised sensitive public sector systems during the shutdown or who may do so in the future as a result of an enhanced shortage of skilled cyber recruits which will leave mission critical roles empty or poorly staffed.

Every breach jeopardizes national security, destabilizes democracy, and results in the exfiltration of sensitive PII, intellectual property, and state secrets. It is irresponsible for our legislators, national security and cybersecurity community to not consider what major breaches have already occurred as a result of the 2018-2019 partial shutdown that have yet to be uncovered. Have we seen this trend before? Is possible that the 2013 sequestration in some way contributed to the devastating OPM breach? America relies on its current and future cyber talent as an irreplaceable national security defense against nation-state advanced persistent threat (APT) actors, digital terrorists, cybercriminals, and other threat actors.,

Now, due to the impact of the shutdown, the public sector will need to offer significant incentives to attract emerging cyber talent as well as to retain its current personnel. These should include actions that restore confidence in current and future cybersecurity professionals in the security of their jobs such as deeming cybersecurity workers as essential personnel, therefore shielding them from the impacts of any future shutdowns.

The Government Shutdown Impacted Cybersecurity Recruitment and Retention

The government shutdown impacted approximately a quarter of the civilian government and put more than 800,000 federal employees in a state of financial hardship. ICIT Fellow and DLT Chief Cyber Security Technologist Don Maclean explains, “At many agencies, cybersecurity staff are deemed ‘non-essential’ employees, and are thus on furlough during the shutdown. It is hard to determine the precise impact of their absence, but it is certainly significant, and grows more serious each day. It is time for cybersecurity to take its place along physical security as an essential function of the Federal government.” Many reported feeling like undervalued pawns in a political game. Worse, many early career cybersecurity professionals who were already accepting lower salaries than their counterparts in the private sector have been instilled with a sense of doubt in their decision to work for the federal government. The government cannot afford to lose any cybersecurity professionals; let alone young talent who may be more adept at navigating emerging technologies [1].

During the 35-day government shutdown, about half of the Department of Homeland Security's main cyber agency staff was furloughed; meanwhile, the other half were required to work without pay. In an interview, Senator Ron Johnson, who chairs the Senate Homeland Security Committee, stated: "This is not helping the federal government's ability to attract and retain people in some very important positions that require a fair amount of sacrifice." In the week following the shutdown, Johnson expressed concern that in the near future, energy plants, airports, and other critical infrastructure organizations would not be able to secure their networks against sophisticated cyber attackers due to cybersecurity workers aversion to accepting or retaining government jobs rather than pursuing employment in the hire-paying private sector. Recruiting and retaining cyber talent was already an insurmountable challenge for the public sector since highly skilled workers may be able to earn as much as two or three times their government salary in the private sector [2].

These sentiments were echoed by many in the cybersecurity and national security community in a bipartisan manner, and supported by a look at statistics on cybersecurity jobs in the metro D.C. area. Around the end of the shutdown, CyberSeek.org reported that the D.C. metro workforce contained 6,226 cybersecurity public sector workers and 3,709 unfilled cybersecurity positions. At the same instant, 40,349 private sector cybersecurity positions were available in the immediate area.

While the race for cyber talent recruitment is not a new concern for the public sector, the already dire predicament was exacerbated by the shutdown because:

- Recent hires and experienced agency professionals alike may no longer view public sector employment as reliable.
- The risk of periodic unemployment combined with the already lower salaries is a significant economic disincentive for emerging talent.
- The sheer volume of private sector cybersecurity jobs and fewer barriers to entry such as faster hiring cycles are attractive to prospective employees

Existing Personnel May Feel Disenchanted With Federal Employment

According to a federal agent of more than 20 years who spoke with Brian Krebs, the talent drain resultant from the shutdown is predicted to set the federal government back by as much as five years [3]. Cyber personnel who missed multiple paychecks, some of whom continued to work in the interim, may evaluate their other options such as retiring in the near future or seeking employment in the more lucrative private sector. Investigators and agents could not retire during the furlough because they could not be processed out; nevertheless, it would not be surprising if the federal government reports record high retirement rate of civilian personnel in the next several years, especially those from technical and cybersecurity backgrounds. For 35 days, national security cyber missions went unfunded, investigations went without resources, and intelligence sources were disengaged [3]. Returning employees were met with significant backlogs of threat alerts and log files. The feeling of inundation may not sit well with the current workforce [4].

The mental and morale repercussions have made many feel undervalued and in some instances, desperate. Many agents and other public sector employees reportedly sought side jobs despite rules restricting such activity [3]. Having to assume a second job because what was supposed to be your stable job with a steady paycheck and unparalleled benefits became unreliable, is a humbling experience, but it may also prove to be a disheartening and disenchanting one that persuades existing cybersecurity personnel to cease protecting America against digital threats from within the government and instead choose to do so from the private sector.

Emerging Talent Will Be Hesitant to Enter the Public Sector

If existing personnel exit the workforce, the public sector will need to rapidly recruit fresh talent to defend critical systems from adversarial compromise. This is already a daunting task for the public sector which has now been exacerbated due to the shutdown. ICIT Fellow and Simon Data Chief Security Officer Robert Wood summarized the impact on future cyber talent recruitment as, “I believe that the shutdown will further entrench the belief of many in the private sector that going to work for the government just isn't worth the headache. If it's already a decreased salary with a huge increase in red tape but now there's a risk that you may need to go without pay because of politics, that's a big disincentive for talented people to stay in the private sector.”

Emerging talent do not possess the same qualms as previous generations about changing positions or career paths because they are saddled with excessive student loan debt, and they have been repeatedly told by the media, their parents, and members of other generations that due to the state of the economy, millennials will have to change careers often in order to maintain consistent employment. These young hires are not far enough in their careers to have built up a retirement or otherwise feel locked into a government position, especially when the federal government deems roles in cybersecurity as non-essential. For those in the Information Security field, who feel that everyday their work helps to secure America's critical systems and vital data assets from adversarial compromise and exploitation, being deemed non-essential sends a clear and devastating message that cybersecurity, and the cybersecurity professionals who guard the nation against enemy nation-states, cybercriminals, digital terrorists, and other threats, are not seen as necessary to the nation's lawmakers and leaders [1].

The recent shutdown, the sequestration of 2013, the potential for future shutdowns based on the precedents set by partisan politics, and a continuous feeling of uncertainty and underappreciation will inhibit future cyber talent from working for the federal government because for many the main draw to a career in federal cybersecurity was the stability and reliability inherent in the position. There was a belief that working for the federal government was a reliable job with a reliable paycheck. That dream may now be gone. It was proven a gossamer illusion. Given recent partisan developments, would you recommend that your brother, sister, son, daughter, or grandchild seek employment in the public sector?

Recent college graduates seeking employment will hesitate before accepting a public sector position that promises exceptional training and the exposure to bleeding-edge scenarios, over a private sector position that offers nearly 30 percent more pay and is now seen as more dependable.

How Can America Retain and Recruit Cyber Talent

In a January 28, 2019 letter to Homeland Security Secretary Kirstjen Nielsen, Senator Mark Warner, ranking Democrat on the Senate Intelligence Committee, expressed that "shutdowns like this one have the effect of discouraging talented individuals from joining the Federal workforce, and [push] some of our best toward alluring careers in the private sector" [2].

While avoiding government shutdown altogether is the most ideal solution to retaining and recruiting cyber talent, the government needs to immediately implement practical policies that will create confidence, trust, and incentive among current and future employees. . These may include:

Elevate Cybersecurity Roles to "Essential Staff"

Congress and agencies should recognize the vital role that public sector cyber personnel serve at every level and to re-categorize them as essential personnel so that national security is not jeopardized when partisan disputes disrupt the federal government [2]. This will alleviate concerns among employees about the stability of their paychecks and arm recruiters with a stronger message when competing against private sector offers.

Raise Salaries to be More Competitive

Senator Johnson suggests that the Senate take measures to raise the salaries for federal cyber professionals and offer more flexibility to move from agency to agency to share their expertise and gain new skills. Johnson also said he plans on creating a fast track for civilian government cyber professionals to rotate between agencies. A similar bill was introduced in December

2018 by Senator Gary Peters. The goal of Peter's program was to "boost collaboration between agencies" and "enhance their careers and broaden their cybersecurity expertise" [2].

Be More Collaborative

Just as Congress should be more collaborative to avoid future shutdowns, agencies must become more flexible with regards to the exchange of cyber talent. Some cyber security professionals eschew the public sector because they either fear getting locked in to a "dead end job" or they feel stifled by bureaucratic red tape that prevent them from securing critical systems. In the private sector, one has the freedom to accept or quit any job. The federal government needs to offer a similar measure of freedom. To alleviate these frustrations and tribulations, agencies should increase the number of rotational programs offered that enable cyber talent to freely move between projects and agencies, allowing for reasonable notice and applicable clearance procedures.

Conclusion

America depends on its cybersecurity personnel to defend its digital space as much as it depends on its military, law enforcement, and other personnel to defend its physical territory. Congress would be remiss to fail to deem the nation's cyber staff as essential personnel. To retain and recruit talent, federal agencies need to consider measures including increasing the pay and benefits offered to cybersecurity professionals to be competitive with private sector organizations, instituting flexibility in the inter-agency exchange of talent, and other incentives to build trust, confidence and incentives to attract and retain top talent in today's hyper-competitive human capital environment.

Sources

[1] Trexler, E. (2019). The Shutdown's Impact on Cybersecurity Talent. Retrieved from https://www.nextgov.com/ideas/2019/02/shutdowns-impact-cybersecurity-talent/154535/

[2] Marks, J. (2019). The Cybersecurity 202: This is the Senate Homeland Security Committee's top cyber priority this year. Retrieved from https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/01/31/the-cybersecurity-202-this-is-the-senate-homeland-security-committee-s-top-cyber-priority-this-year/5c51d8ce1b326b29c3778d1f/?utm_term=.64baef024bc2

[3] Krebs, B. (2019). How the U.S. Govt. Shutdown Harms Security — Krebs on Security. Retrieved from https://krebsonsecurity.com/2019/01/how-the-u-s-govt-shutdown-harms-security/

[4] Callahan, J. (2019). What the Government Shutdown Teaches Us about Cybersecurity - Dark Reading. Retrieved from https://www.darkreading.com/what-the-government-shutdown-teaches-us-about-cybersecurity/a/d-id/1333836