Government Business Council

HUNTING TOMORROW'S THREATS

A CONVERSATION ON SECURITY MODERNIZATION PRIORITIES

splunk>

EXPERT DIALOGUE

INTRODUCTION

Security modernization strategies are top of mind for government IT experts. With cybersecurity threats like SolarWinds, and new guidelines set out by the Biden administration's May 2021 Executive Order on cybersecurity, federal agencies are re-examining their modernization priorities and evaluating where they stand. What steps have already been taken? What remains to be done?

To explore those questions, Government Business Council conducted a qualitative research study capturing key insights from experts in security modernization across the federal government and DOD. Interviewees are:

THE EXPERTS

Shane Barney
Chief Information Security Officer
U.S. Citizenship and Immigration Services

Renata Spinks
Assistant Director of Information Technology/Deputy CIO and Senior Information Security Office
U.S. Marine Corps

THE INTERVIEWS

What steps has your agency already taken towards modernizing your cybersecurity posture?

SHANE BARNEY

In the early 2011 and 2012 timeframe, we got a new CIO who stepped in, Mark Schwartz, and he had two big goals. He wanted to implement agile methodology development, and he wanted to deploy to the cloud. Adopting those principles of agile development forced us to move into the cloud and develop a modern stance in how we approach security. Agile development is a very different process. In the old days of security, we were very compliance focused, policy driven, everything was done with gates and these massive waterfall projects. Security had all the time in the world to look at things and keep the tires on things. Two years between releases was not unheard of. Modernization was driven by events. It wasn't just something that sounded good. It became real world for us. Frankly, we were doing it at a time when nobody else was. USCIS was the first to go to cloud in the Federal space. I'm sure we were the first to use agile practices.

That's how we got into modernization. It was more of a forced thing. It was hard for a lot of people to adapt to it — our approach to security was so radically different that most people couldn't wrap their heads around it. We started looking at things and accelerating the way we were doing things to focus on true risk management, instead of lukewarm box checking.

RENATA SPINKS

The Marine Corps is everywhere. We are located in the Pentagon, the United States, and even overseas, but there's areas where we are deployed that we are either in other countries with different operating authorities, or we are in disconnected or very limited bandwidth environments, or in a zone or a situation where connectivity is based on customized networks like satellite communications. So modernizing our security posture has to consider all those different environments.

The Marine Corps is committed to Force Design 2030 and Naval integration. These two topics are about resiliency, security, and agility. If we don't have the security, agility and resiliency from a capabilities' perspective, then we're going to have some challenges. We have a network modernization plan that's amended with a couple of roadmaps depending on capability. We are involved with the acquisition community and different partners in industry who are providing not only capabilities, but sometimes designs.

While that's the operational side, my favorite topic is the governance piece around our cyber security modernization structure and posturing. If we don't have the governance in place, then it slows us down on our operation side because our operators don't really know what's expected of them. In that future year defense program, that includes cybersecurity posture from a system and systems approach, meaning cloud. You hear a lot about that. You hear a lot about zero trust. But we also have free space optics. We're looking at 5G. We're looking at secure application development at the edge, and when we say tactical edge, those spaces where we've created networks and connectivity focused on security. Oftentimes that defense in-depth approach can't be realized with just a commercial connection.

We have a lot going on, but in order to posture the service for our modernization priorities and to make sure we're doing the best in the cybersecurity perspective and determining where to accept risk, it's been an area of focus to engage with others outside of our day-to-day workplace so that we truly get a whole of service picture. So often we focus on our normal day-to-day business operations' perspective, and so often the weapon system side and the actual warfighting and the technologies that we employ goes overlooked.

What do you see as challenges your agency is facing on your cybersecurity modernization journey?

BARNEY

Security challenges have remained, in the sense that we continue to move forward. Now the move is towards microservices. Microservices defy all things in federal security IT. They are not systems or data holders. They present so many different challenges that it's a unique opportunity to change the landscape for the better, towards a different type of approach to security in something I've started referring to as baseline security.

The idea with DevSecOps is that you build in security as you develop, but baseline security in a microservices world means you have to build it in at the very base core of the infrastructure. Everything then inherits up from there, because each little piece of a massive application can be individually developed and deployed irrespective of the other pieces and parts.

In CIS we're heavy in immigration, obviously. Take things like intake. How do we accept information from the public to facilitate the immigration process? That's something that everybody in my organization needs as a domain. How do you provide information out to the public? You have to provide notifications. That's a domain. So you create business domains, and then the microservices are built around and within those domains to support them. It's a system-less approach to doing things, and it's exceptionally challenging from a security standpoint. Because, if you do it wrong, if you don't include some aspect of the architecture that's important, it proliferates through your entire environment. It's not just going to affect a single system. It's going to affect everything. It's really critical for us to get that security right. That also means investing really heavily in automation. Automation is going to be our saving grace, which is something USCIS started doing a very long time ago and has had considerable success with.

SPINKS

There are two areas of challenges. The first one is integrating technology for the warfighter, no matter where they are. The largest challenge is at the tactical edge. Warfighting is hard. Using technology that's supposed to operate in highly denied, disrupted, intermittent or latent environments [DDIL] is the biggest challenge. How can we have the capability that positively impacts our business mission areas, but we sub optimize in the connectivity environment? Even though that's a challenge, we see those as opportunities that we're partnering with industry on today.

The second one is the impacts of technology accelerations. We're consistently seeing new technologies and we're consistently seeing new products and new features. That's great, as we look at the way our partners in industry are finding better ways to use technology, but that modernization requires a large scale investment for us. Employing some of the things that we could really see benefit from is particularly challenging as we migrate to the cloud right now, because delivery models change, the technology changes, but it changes at a pace that's not aligned to the government's budget cycle. Oftentimes the technology that we're looking at employing comes out during an execution year, which means we haven't budgeted for those technologies. Part of that acceleration and modernization piece is how we capitalize on those efficiencies within the budget cycle wherever it's possible so that we can have a little bit more efficacy in the way we spend.

What do you think would it take for your agency to be able to reach the next level of modernization?

BARNEY

From a business and IT at large leadership, I think we've got what we need. In order to do good domains, you need the basic structure of it, which we've already done. You need a governance process behind it. That surprises a lot of people, who think that agile methodologies and DevOps tend to be less governed. Microservices and domain driven design really rely on it, because you're bringing together, in a very close relationship, the business and the IT units. You've got to make sure that your governance processes are lockstep in doing so. USCIS spends a considerable amount of time developing that next generation of governance and really working out how leadership at the very highest levels can be involved in helping us make good IT decisions based on this domain driven design. That's really critical for us. There's lots of little elements beneath that all feed up, but it's very key that you control that piece, because it'll just spiral out of control.

SPINKS

I think our network modernization plan and our criteria for measures of effectiveness and performance help align resources and prioritization. Oftentimes we go after the shiny new object, but we don't necessarily focus on everything it takes to occur on the network or within your information environment to enable those features. Our industry partners and people who are fielding new technologies have to go through the FedRAMP process, or process that authorizes the technology to be utilized within the Department of Defense. As long as we continue to look at the assessments and create those criteria to measure effectiveness and then respond to them in the ways to where we can actually drive change, that's going to get us to that next level.

That last piece to help us reach that next level is our deployed mix-in, often referred to as D Mix-in, and that's enabled by our network modernization. It gives the commanders the ability to rapidly deploy with enterprise services, command and control applications, and cybersecurity protections. That allows our network to provide seamless access to information and command and control the ability to make decisions in real time using real time data, no matter where the Marines are located. We're always about measuring efficacy, but creating those concepts of employment and doing exercises so that we can do assessments, understand a real life simulation, and then go back and learn from it to make sure that in those realistic training environments we get as close to reality as possible, and then incorporate what we're learning into those designs.

What do you think are some of the top cybersecurity threats facing your agency, and how are you planning to address these?

BARNES

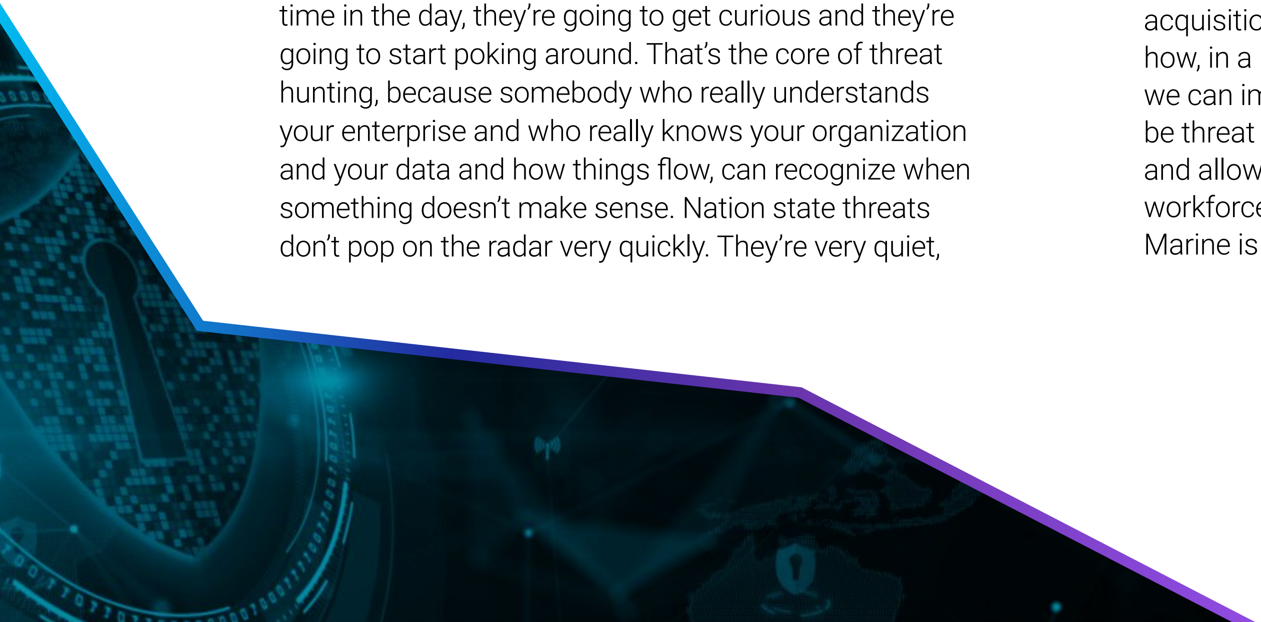
We are a Federal agency, we are part of DHS, and there were impacts from SolarWinds, like everybody else. The risks remain the same from a cybersecurity perspective. But if we do base level security right, it will help us remove known risk. We know that that risk exists and we know that we have to mitigate it. You can mitigate it through a manual process, check a box off and be good to go, and then issue an ATO and wait three years. Or you can automate it. If something happens related to this risk, I'm going to get an alert. Fixing it is, if at all possible, going to be automated as well.

We had a couple really close calls, no exposures, but close enough that it scared us. We sat back and realized that there was no way for my people to sit there and stare at screens and monitor that. Why don't we just automate it? It was really the first time we automated

something from a security perspective. That's how you deal with risk. The challenge with base level security is automating all that risk out of existence, and then focusing on what you don't know.

If we took any lessons learned out of SolarWinds, it's that you can check all the right boxes. You can be in complete compliance. But at the end of the day, it didn't matter that we were in full compliance. It mattered that we didn't know something was going on because we weren't looking. What baseline security, domain driven design, and microservices are really doing is driving us towards a threat hunting based type of operation. In other words, you're going to automate out of existence, all your known risks and in place of that, this threat hunting mindset will take over.

Once that happens, you begin freeing up your own internal resources so that those resources at all levels become part of your threat hunting organization. If you employ really smart people, and you give them time in the day, they're going to get curious and they're going to start poking around. That's the core of threat hunting, because somebody who really understands your enterprise and who really knows your organization and your data and how things flow, can recognize when something doesn't make sense. Nation state threats don't pop on the radar very quickly. They're very quiet, very stealthy, so small and so well hidden that you miss them in the general picture of things. So ending the perception of your organization's security and moving towards something that is far more threat based and more data driven is going to be the future. It has to be.



SPINKS

The greatest threat to our network is expanding the portfolio of technologies, and so when we talk about network modernization and cybersecurity, let's be threat informed. How much of the new normal do we adopt, and will it go back to the way it was? It probably won't, because the threat hasn't changed. Actually, the threat has gotten larger. That's why the executive order focuses on zero trust and making sure our credentials and access management are in place. If we don't do that, if we go back to the way we did things in the past, then that cyber security threat is going to "eat our lunch."

It will continue to help us improve on the way we do things. In the Marine Corps, we're looking at our acquisition and defense industrial base and figuring out how, in a resource-constrained, cyber threat environment we can improve the cybersecurity posture and have it be threat informed across the Department of Defense, and allow those two areas to feed how we manage our workforce and how we deploy, no matter where the Marine is accessing that capability.

In what way did the COVID-19 pandemic affect the way your agency approaches cybersecurity protocols, if at all? Do you think that these changes will remain part of your cybersecurity posture?

SPINKS

It didn't change our approach or strategic intent. It changed the how. For example, we look at our dev tech ops approach. Of course we want the continuous monitoring and diagnosing in place and diagnosing, and to get to a point where our applications are modernized and outside of our Marine Corps data centers as part of the Cloud so we can take advantage of high-performance computing and decision making, and cost avoid in the areas of storage and maintaining those abilities. When COVID occurred, our developers were very accustomed to interacting with each other, in a collaboration room and talking to each other. Well, that went away. That was the largest impact. How we engage with each other changed in response to COVID-19. It didn't affect productivity, but the effectiveness of the productivity and our ability to make decisions was sometimes affected in a negative manner because the way we were accustomed to operating changed so much with a distributed workforce working from home. That introduced all kinds of security challenges that we had to address. The stop move and the reduction of force that you started to see across the United States as a result of just trying to keep people in quarantine, that started to go from 40 to 50% manning to sometimes 10%. You can imagine if it takes 50 people to man a command operation center or network operating center, or if it takes three people to generate reports and pull together briefings so that we can communicate statuses, and then that force all the way down to one person, you could see how that would be a challenge. I think that's an area that we will continue to take advantage of, but we're not out of the woods from a perspective of the how.

What is on your personal "wishlist" for your agency's cybersecurity journey? What would be most helpful to you in your role?

BARNEY

If we're really going to do true modernization of security, it's got to go beyond just my level or agency level or even the department level. We've really got to look at FISMA. The last update was in 2014, and back then people still were trying to understand what a cloud was, much less anything else. The world has changed considerably. We have a business doc to be kept up to speed and changed as well. There's a number of bills in Congress right now pushing forward and they're looking to insert a lot of changes. Some of those changes need to be explicit rules that are explicit powers and authorities given to CISOs for example, and delineating out their operational role. They've got to be more than policy shops. So many of them tend to be that, or at least looked at that way. We need to start driving that operational requirement. They need to be part of the solution. I've always seen security as a driver of mission, not a detractor. We need to reincorporate that notion back into FISMA. It's critical to success here, and I know there's a lot of talk about it.

I hope that the powers that be will start recognizing the importance of changing the dynamics of the CISO and CIO roles, and how those would be affected in the larger set of the organizations that they operate in. It's going to be critical to success in the future.

SPINKS

I talk a lot about the people, because if we don't invest in our workforce, you won't be able to say that you value your workforce because you're not investing in them, right? You can't take advantage of all that we, as a people and a culture, bring to the fight. The Marine Corps is known for lethality, but if the weapons that we use and the hardware and software are not able to be employed correctly, then we're not lethal. In order to do that, the people have to be trained. We have to be able to recruit and sustain Marines, whether that's civilian Marines, active duty, or reserve. My wish list is focused on recruiting highly qualified experts. We're evolving the learning infrastructure. How can I support the workforce and continue to invest in the workforce and make sure that we can frequently adopt new technologies, and train our workforce? Oftentimes we're so mission focused that we allow our individual development plans to be all about achieving the mission and while that's great, the job satisfaction for a work/life balance is really where I put a lot of my energy in. If I am dealing with a workforce that's happy and satisfied and that they understand that the mission still has to get done, my experience has been that they're going to give all that they can in a culture and in a workforce that supports them and values them. We often take for granted what is there, but I think COVID-19 forced us to recognize how much we really yearn for the relationships of people.

SPLUNK'S PERSPECTIVE

BILL WRIGHT, SENIOR DIRECTOR, NORTH AMERICAN GOVERNMENT AFFAIRS AT SPLUNK

The fact sheet accompanying the Executive Order appropriately noted that Recent cybersecurity incidents such as SolarWinds, Microsoft Exchange, and the Colonial Pipeline incident are a sobering reminder that U.S. public and private sector entities increasingly face sophisticated malicious cyber activity from both nation-state actors and cyber criminals. Since the order's release in May, we have not seen any decrease in the sophistication and frequency of incidents.

One important lesson that emerged from the COVID-19 pandemic was the relationship between IT modernization and resilience. Agencies that were established in the cloud remained nimble and resilient during the pandemic. Those that were still nursing their legacy systems floundered under the surge in demand of remote work and providing remote services. The pandemic forced the private and public sector to confront outdated beliefs and baselines that were based on instinct and experience. Because it was disruptive both operationally and programmatically, it caused organizations to ask deep questions about how the government delivers on its mission. It's these types of questions born out of necessity that drive innovation.

As a trusted federal partner with decades of experience, we thoroughly understand Federal ecosystems and the cybersecurity challenges that leaders face. We are prepared to enhance federal capabilities to both empower missions and support a modern federal government. We're exceptional at improving detection, investigative and remediation capabilities - Splunk SOAR empowers agencies to automate alert triage and repetitive security tasks that bog down security operation center (SOC) personnel.

Data, and our ability to understand what it is trying to tell us, plays the central role in many of the administration's cybersecurity priorities. In addition to logging standards, Splunk plays a crucial role in a zero trust architecture -- a data-centric approach to security that assumes an organization has already been breached and works to limit an adversaries movement. As a recognized leader in log management and SOAR, we've furthered our commitment to strengthening our national cybersecurity posture by designing packages solely for federal agencies to address the requirements around cyber incident response per the Biden Administration's recent executive order, OMB M-21-31.

We are proud to announce the recent launch of our Splunk Government Logging Modernization Program to further equip U.S. government agencies to meet cybersecurity requirements. Splunk is providing the following as part of its Government Logging Modernization Program:

- New Splunk Cloud FedRAMP Packages & compelling programmatic pricing exclusive to Federal Agencies - helping to lower cost, accelerate compliance, and improve cybersecurity resilience;
- Expanded storage options with lowered costs, enabling customers to accelerate investigative and remediation capabilities through enterprise log retention;
- Comprehensive Splunk Cloud FedRAMP migration assessment and customized services to help agencies rapidly modernize their logging program; and
- Assigned Security Expert services to guide our customers through the cloud maturity path and help agencies navigate the requirements outlined in logging maturity model stages EL0-EL3.

At Splunk, our highest priority is to help our customers create the right data strategy for their cloud journey and they trust us to manage their increasingly complex technology environments and equip them to drive better data-informed decisions, faster. We play a key role in helping our customers accelerate cloud-driven transformation by not just migrating applications, but by providing end-to-end visibility and giving them the ability to unlock new insights and act on all data across every stage of their cloud journey to better serve their mission. Whether it's managing costs, ensuring resilience, securing what matters, releasing faster or capturing the value of data, our platform and purpose built solutions are the data backbone for modernization.

ABOUT GBC

As GovExec's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of GovExec's 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

Learn more at: govexec.com/insights

ABOUT SPLUNK

Innovation takes many forms: transformative business changes and incremental optimizations. Both types of innovation are predicated on having secure and resilient systems. With Splunk, customers efficiently ensure security and resilience, freeing up resources to identify opportunities in their data and deliver innovations, even in the face of unpredictability.

Learn more at: https://www.splunk.com/