Mobility and the Government Challenge

Privoro's Campbell on the Need for Empowering a Mobile Federal Workforce

iSMG
INFORMATION SECURITY MEDIA GROUP

PRIVORO®

Federal government agencies face unique cybersecurity risks. As a result, they often place tight restrictions on mobile devices in the workplace. **Michael Campbell** of Privoro says it's time to loosen these restrictions because they are negatively impacting missions, recruitment and retention.

In an interview with Tom Field of Information Security Media Group about empowering the mobile federal workforce, Campbell discusses:

- Unique mobile risks and threats in the federal arena;
- How government restrictions on mobile devices impact mission and recruitment;
- New strategies to mitigate mobile risks.

Campbell leads Privoro's government and federal business. Previously, he spent more than eight years with Cisco helping create and run the company's largest government partnerships. Earlier, he served as an Army signal officer for 13 years with deployments in over 20 countries, including Afghanistan and Iraq. He also served as chief of staff for the Army's CIO, helped write the strategy for the Army's Global Network Enterprise Construct and served as a military legislative assistant for Senator Conrad Burns of Montana.

Sizing Up the Risks

TOM FIELD: Michael, what do you find to be the unique risks and threats to the federal government mobile workforce?

MICHAEL CAMPBELL: The easy way to answer that question is to step back and think about the risks that commercial mobile devices place upon the users. Today, the commercial mobile devices that are in use are truly wonderful devices. They have hundreds of billions of dollars of developmental work that has gone into the development and creation of this amazing platform. They are capable of doing a lot of things.

Because of that, the phone manufacturers and the app developers have access to a lot of information that these wonderful devices give them.

The devices have cameras that can record from the front and back and they have microphones. Most people don't even realize how many microphones are on a mobile device. They range from anywhere from two to as many as five on a given platform. And in some of those cases, those microphones are for the exclusive access of the actual phone manufacturer themselves.

Michael Campbell

So anyone working in government is at risk of disclosing sensitive information. Everyone is dealing with something that could be sensitive. If they, in the course of their work, have a commercial mobile device and they never know if it's on or off, then that device could disclose or be leaking information either to these overreaching app developers or to someone that has gained access to your device for nefarious reasons.

And in the aggregate, that data becomes quite powerful. For example, a recorded conversation … can be translated to text, and then a keyword search can be conducted and then the data can be aggregated. And then the collection of all that gives away quite a bit of sensitive information.

Anyone who has a very sensitive role … is at even greater risk. And because of that, restrictions have begun to be put in place.

Most people say, "Ah, there's just really not that many people that work around sensitive information." But at least 96 separate agencies have special agents that were law enforcement arms where they're out doing active investigations or they are doing confidential type work. That's basically the entire federal government. … So you can't say, "This is a DOD problem or this is an intelligence community problem." The reality is it's a problem that's across the entire federal government.

Leveraging Mobile Tech

FIELD: So Michael, how would you say that the government sector is leveraging mobile technologies differently than what you see in the private sector?

CAMPBELL: In government, what normally happens is agencies will issue a device. They're embracing mobility and the need for mobility in some way, shape or form. But instead of letting you use a personal device of some sort, they say, "No, no, no. That's too risky. I must have some control." So they'll issue a device.

In other sectors, bring your own device is allowed. Then you sign some agreement that gives you access to your company or commercial assets and services. But in government, you've got to have a government-issued device. That way, the government has greater control over that device.

If you work for the government, you'll get issued a device, you'll have a service plan that supports that device and this gives you the ability to be reachable while on the move. There are easily hundreds of thousands of devices issued to employees in the federal government. The Government Services Agency has provided over 100,000 devices to every agency. The last time they did an actual audit, they could account for over 3 million service plans that had been provided inside the federal government.

Consequences of Restrictions

FIELD: So Michael, I know that some government agencies actually restrict the use of mobile devices. What are the immediate consequences when that's the policy?

CAMPBELL: There are a lot of devices that are issued, and people are beginning to use them in every aspect of their government job. There is an awareness that this is a risk. So what's the risk? Because there is awareness of these devices being able to listen or take pictures and track other things that you do … there is an ever-increasing lockdown on those devices. If you go to work in an organization that acknowledges a sensitive mission, you're going to see a lockbox sitting outside of the office. And that lockbox is where you'll stick your mobile device and you'll then go to a desk. You won't have access to that lockbox.

What are the consequences of that restriction? Let me tell you a story. We had a gentleman who was in his early 20s, a developer who was used to working on multiple different automated systems to do his job. He's coding. He's checking. He's collaborating. He's doing multiple things to enable an outcome. We brought him in and took him into a government environment where we were doing some stuff and he had to give up everything. He had to give up his mobile phone. He had to give up his tablet. He walked into an environment where no one had any connectivity except for a desk phone and a desktop computer. And he looked super frustrated and he was not really sure how he was going to do the job that we had asked him to do.

> "The real consequence of cutting back or restricting the use of modern mobile technologies is that you're operating like a 1980s organization."
>
> Michael Campbell, Privoro

And another older government employee could sense that he was frustrated and brought over to him a tablet of paper and a pen and dropped it on the desk in front of him. And the young gentleman looked at him like he was crazy, saying "How's this supposed to help me?" And the reason I tell that story is because it is like going back in time.

So the real consequence of cutting back or restricting the use of modern mobile technologies is that you're operating like a 1980s organization. In the 1980s, you might have left the building to go smoke. Today, you run out of the building to use your mobile phone because you have to play catch-up. … It could be because you're doing some work that's easier to accomplish on the mobile device than it is on the tool that is sitting at your desk.

If the government worker is not at work, then we hope and pray they won't discuss something that is sensitive or disclose something that should not be disclosed. But the reality is that everyone self-selects that level of risk and whether or not they're going to share or do something. People go to lunch. People go to remote conferences. People go to work in a remote site. People take phone calls from their cars and declare them sensitive, secure environments. These kinds of things are happening every day.

So there is no real risk mitigation while you're on the move. And then inside the work environment, you're definitely operating in a constrained and ineffective way compared to what you could be.

Impact on Recruitment

FIELD: Michael, following up on the story you told, what long-term impact do you see regarding recruiting and retaining a government workforce?

CAMPBELL: You want to recruit young, bright people into your environment. Today's young, bright people have had a mobile device attached to their hand since they were very little. If there isn't a video screen up when they make a phone call, they think the phone is broken.

> “I’ve never seen a collection of interested parties across government come together on an issue like I have seen them come together around mobility.”

So if you’re trying to recruit a person straight out of college, or someone who’s been out of college for a few years, they definitely would prefer to be in an environment where they can remain connected and leverage the tools that are available to them to be very fast and collaborative.

And if you tell me you’re going to take that away from me, I’m most likely going to go work somewhere else. And that’s happening. I’ve been told that recruiting and retention are seriously down across the entire government and the contractual workforce as well. Because whether you’re a government worker or you’re a contractor supporting government, you’re being impacted by these same restrictions.

And the mission also is impacted. It takes the government forever to do anything. And that is true for many reasons, but one of them today would be that people are just slow to make decisions. They’re slow to get back to you. They’re slow to collaborate with you. I have seen and experienced sometimes days and weeks between communications because I can’t get ahold of someone. They have disappeared during the work day. Their phone is in a lockbox. They’re not at their desk. So how do I get ahold of them to get them to make a decision, to move forward on something, to agree to something? It becomes quite challenging. And that’s a simple mission impact. There are bigger mission impacts as well, but those are ones I want to share.

Mitigating Risk

FIELD: So Michael, what strategy is Privoro seeing government agencies take to mitigate the risks of commercial mobile devices while still allowing their use?

CAMPBELL: That is a good news story and I appreciate the opportunity to share it. I’ve never seen a collection of interested parties across government come together on an issue like I have seen them come together around mobility. We have been at about 16 different government agencies in working sessions to discuss options to move forward to solve the problem. Everyone sees it as a problem, and everyone is anxious and looking for what we can do. That’s part of the good news story.

The other part of the good news story is some agencies, some DOD organizations, some federal agencies are taking steps. The steps are around reducing or mitigating risk.

The first big thing is you’ve got to control camera and microphones on this commercial mobile device. This commercial device was designed to do everything, and it has a very large attack surface and lots of cameras and lots of microphones. I’ve got to somehow disable those things. So they’re taking action with the available technologies to do that.

The other part is they’re gating access to different services so that maybe I have multiple work environments or multiple environments on my commercial device. I have a personal environment and I

“There’s a recognition that nobody really sits at their desk all day anymore.”

Michael Campbell, Privoro

have a work environment. They’re figuring out and leveraging technologies to separate those. And then the other thing is they’re actually investing in the wireless solutions that allow them to govern the data as a person is using their mobile device technologies in the way that you would have done this with fixed infrastructure over the last decades. Today, it’s starting to put those same investments into the wired decisions.

And you’re bringing this entire portfolio together and it becomes a comprehensive solution that says, “Hey, that commercial mobile device, the risks have been mitigated. Go ahead and carry that device. Use that device in the work environment, and then use that device while you’re out doing your job on the move.”

The Benefits

FIELD: So Michael, given the strategy you’ve described, what cost benefit do you think agencies could achieve?

CAMPBELL: There are two ways to answer that question. One is how do I pay for this? What is the strategy to fund my investment? And then what is the implied savings or the expected savings? So the strategy is, there is an existing spend on information technologies. IT today primarily is on fixed endpoints, desktop phones, desktop computers and conference rooms. It’s a massive investment, and there’s a big lifecycling budget that goes with those technologies. What we’re seeing is an analysis of that spend, which is enormous. Some people cost their organization as much as $15,000 a year to sustain their fixed endpoint technologies that they use, that they can only use at their desk.

There’s a recognition that nobody really sits at their desk all day anymore. Everyone’s collaborating in their job. Everybody’s moving. So how do we just shift that investment? Let’s not lifecycle the fixed endpoint solutions. Let’s, instead of lifecycling, let that run to end of life. The end of life on most of those technologies is five to 10 years, so let those things run to the end of life and we’ll shift that investment into a mobile phone, a tablet, the wireless infrastructure – all of the other systems that allow you to put a secure mobile solution in place. That gets you the funding you need.

The second is how do I articulate the savings? And there have actually been numerous different independent studies that all concluded the same thing. If I can give back to the typical government employee ... 30 minutes a day – where they make a decision, where they review a document, where they agree or disagree on something or increase their knowledge about something that’s coming up – the amount of value on that is in the millions, even for a small organization, per year. And employees can certainly get 30 minutes back if they can carry their mobile phone all the time safely, securely. ■

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANKINFOSECURITY® CUINFOSECURITY® Just for Credit Unions GOVINFOSECURITY® HEALTHCAREINFOSECURITY®

infoRisk® TODAY CAREERSINFOSECURITY® Data Breach. Prevention. Response. Notification. TODAY CyberEd.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io