KPMG

# Supply Chain Security

## 3 Helpful Takeaways for Government Agencies

Over the past several months, cybersecurity incidents like the SolarWinds hack and the Kaseya ransomware attack illustrate how malicious non-state actors are working hard to disrupt operations. To ensure the trust and confidence of their constituents, what should government agencies be doing?



For government agencies, digital supply chains help distribute and carry out mission-critical services, including supporting disaster recovery services, **according to KPMG**. A majority of these supply chains exist within hybrid or cloud environments, making them a prime target for remote cybersecurity attacks aimed at disrupting operations. And although current efforts in supply chain modernization have by and large benefited the government and its constituents, many technology leaders are left wondering what they should do to secure their supply chains from future attacks.

That was the topic of discussion during "**Blueprints for a Modern Government: Trust**," an editorial roundtable presented by KPMG and hosted by George Jackson, director of events at GovExec. Throughout the conversation, leaders from across the government spoke about the complexity of managing these supply chains and what others can do to secure their supply chains in the face of growing threats to the government infrastructure.

If you're looking to secure your agency's operations, check out the three key takeaways from their discussion.

1. Establish Processes of Continually Assessing Risk
2. Security Requires Collaboration among Federal, State and Local Agencies
3. Threats Start at the Individual — Train Employees to Recognize These Threats

KPMG


© 2021 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# 1 Establish Processes of Continually Assessing Risk

Even though government agencies are at a heightened risk of cybersecurity attacks, it's impossible to completely safeguard a system against threats. Instead of hyper-fixating on securing the entire system, agencies should instead look to understand their risks and establish methods of addressing these risks via workflows or processes when possible.

"Most organizations have system integrators, they're buying hardware or cloud services, they have service providers that are providing professional services – any or all within the supply chain can present a risk to the environment," said Kathy Cruz, Director, Government Cybersecurity practice, KPMG LLP.

"And it's not so much the ability to eliminate the risk, which may not be possible, but to know the risk and mitigate it where possible."

For government agencies, determining what information may be at risk is challenging, as there is the tendency to view everything as high-priority, mission-critical information. However, Luwanda Jones, Deputy Chief Information Officer for the Office of Strategic Sourcing at the Department of Veterans Affairs, reminds colleagues that risk assessments should be analytical.

"We have got to be in a position where we can identify the high-value assets and the critical data needed for those high-value assets so that we can put a risk-based decision matrix around that in order to make supply chain, risk-based decisions in order to ensure that we're looking at this from a cybersecurity perspective," she said.

Albeit, Jones does go on to say that although matrices help establish processes of assessing risk, agencies "cannot do everything," and should look to collaborate with others in establishing security best practices. And as recent events targeting local federal agencies show, collaboration is growing in importance.

> "It's not so much the ability to eliminate the risk, which may not be possible, but to know the risk and mitigate it where possible."
>
> **Kathy Cruz**
> Director, Government Cybersecurity practice, KPMG LLP

KPMG

© 2021 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# 2 Security Requires Collaboration among Federal, State and Local Agencies

In the past year and a half, Susan Kellogg, Chief Deputy State Chief Information Officer for the State of North Carolina, saw an "awful lot of threats extending down to the local level." Over the past several years, numerous cities and counties across the globe were hit with costly ransomware attacks, totaling **$233,817 on average per attack**. For state and local governments, each incursion costs taxpayer dollars and hampers the locality's ability to deliver services.

With this in mind, government leaders should look to build collaborative relationships across state and local levels, said Erik Avakian, Chief Information Security Officer for the Commonwealth of Pennsylvania.

"By doing more partnering, collaborating, sharing [of] threat information, and working again with our partners and then bringing those capabilities to our local government partners, we can then succeed," he said.

When state and local governments reach across the aisle to form these relationships, they are by proxy building trust within the greater federal ecosystem. And in constructing a synergistic federal ecosystem, municipalities and state governments create a holistic security posture that can help quickly protect the entire supply chain as opposed to the individual fiefdoms.

"Don't go it alone . . . it's a new frontier in terms of collaborating, sharing, working together and not competing with another state or agency anymore," Cruz said.

**Ransomware attacks**
on average cost approximately
**$233,817**
per attack

KPMG

© 2021 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

# 3 Threats Start at the Individual — Train Employees to Recognize These Threats

Government agencies have long struggled to find enough qualified talent to adequately protect or address the cybersecurity challenges agencies face. Threats like Draytek, F5 BIG-IP and Citrix ADC Authentication Bypass are new, high-profile threats current cybersecurity experts grapple with.

For government agencies, there simply is not time to hire new candidates and hope they can combat these emerging threats. Instead, according to Jones, government agencies must look at training and retooling qualified individuals first.

"On the personnel side of the house, I think the whole federal government has a problem with keeping up from a cybersecurity personnel perspective . . . We need to be training our staff, because we're not going to grow people overnight, but what we can do is train our current staff in the processes and procedures that we need from a supply chain risk management perspective," Jones said.

Furthermore, to take Jones' sentiment one step further, Kellogg highlighted how the burden of cybersecurity shouldn't be solely upon federal tech teams' shoulders. Rather, government organizations, by and large, should start informing all employees about how cybersecurity is a shared responsibility.

"The thing is, is that it's no longer this group of people or the security experts' [concern], security is going to be a part of everyone's job," Kellogg said.

To bolster cybersecurity throughout the organization, government agencies can institute basic employee-centric training programs designed to teach best practices and help employees notice the most common signs and symptoms.

"I think building that pipeline of people and building an education program throughout our organization and throughout the state, to keep people mindful, because we know that the threats start with the individual, that's extremely important," Kellogg said.

> "The thing is, is that it's no longer this group of people or the security experts' [concern], security is going to be a part of everyone's job."
>
> **Susan Kellogg**
> Chief Deputy State Chief Information Officer for the State of North Carolina

KPMG

© 2021 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Want to learn more about how KPMG can help your agency improve supply chain operations?

**Learn More** →

Interested in Watching the Next KPMG TV episode in the Blueprints for a Modern Government series?

**Check it out** →

Back to the content

**Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.**

© 2021 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.