Meeting the Requirements of the Supply Chain Imperative

carahsoft

govloop

Contents

Carahsoft and GovLoop have partnered to provide resources around the latest federal, state and local supply chain initiatives and legislation. The goal is to guide government leaders and stakeholders interested in strengthening their cyber supply chain strategies.

Executive Summary

IT modernization ranks as a top priority for the federal government, but it also further complicates how agencies manage the risks to their cyber supply chains, a concern they've faced every day for decades. IT modernization adds more third-party providers to the mix, creating increasingly complex supply chains for agencies to monitor. The subsequent balancing act can leave agencies struggling to avoid security threats and modernize their IT at the same time.

IT supply chains are the systems that move IT products or services from suppliers to customers. Managing IT supply chain risks becomes increasingly important when you consider the cost of cybersecurity failures. Because IT supply chains contain activities, information, organizations, people, and resources, they're bursting with possible security vulnerabilities. In terms of federal IT supply chains, security missteps can damage the economy, national security and even public health.

In May 2019, President Trump issued an executive order underscoring the danger the federal information and communications technology (ICT) and services supply chains present to the U. S. Trump's order prohibited agencies from using technology and services from any party related to America's foreign adversaries.

Four months later, the Cybersecurity and Infrastructure Security Agency (CISA) published a report identifying nearly 200 security threats to these supply chains. CISA's list included hazards such as counterfeit components, poor product designs and malicious hardware and software. If exploited, these types of vulnerabilities could disrupt public services, cause unexpected costs for agencies and erode citizens' trust in their government.

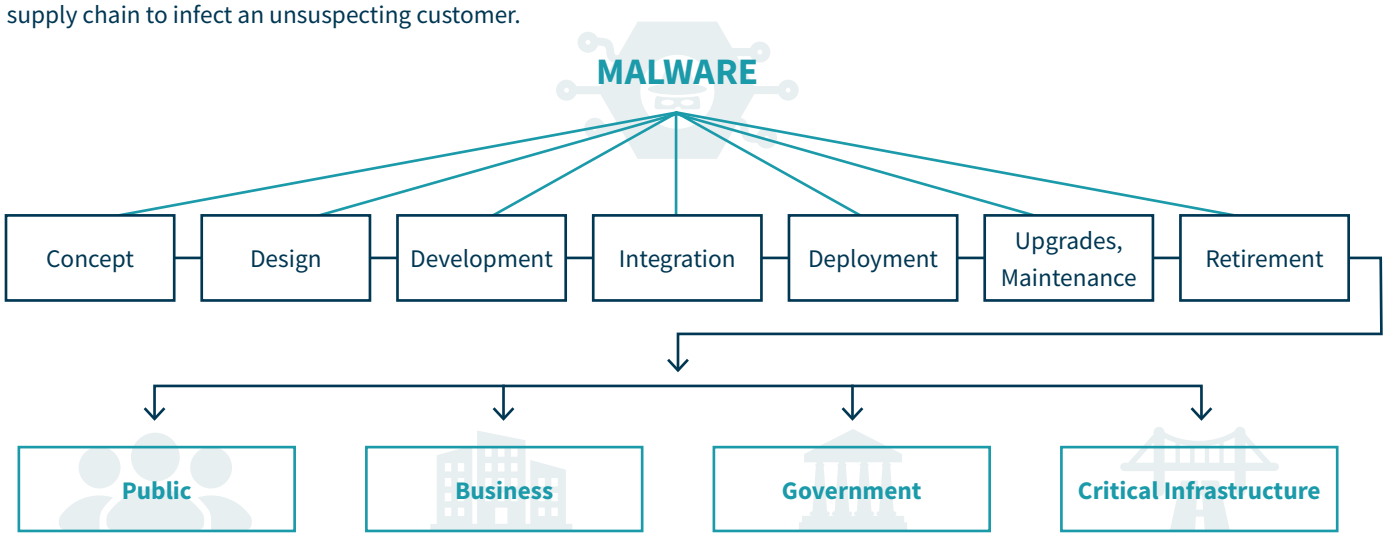
If your agency is straining to juggle supply chain risk management and IT modernization simultaneously, GovLoop and Carahsoft are here to help. This guide can help your agency thread the needle between modernization and security. With case studies, research and interviews with government thought leaders, the following pages can assist your agency with navigating these crucial issues.

- First, we'll look at how risk management for federal ICT and services supply chains is evolving, and explain what these topics are and where they're heading next.
- Second, we'll discuss how agencies can manage their supply chain ecosystems better so they don't sacrifice security for modernization. Not only will we detail why security and modernization matter, we'll also explain how both influence supply chains.
- Third, our guide will illustrate why agencies need full visibility into their supply chains for tomorrow's technologies. Agencies that see their supply chains clearly are better prepared for the latest digital cellular networks and other potentially transformative tools. Ultimately, government agencies that secure their supply chains can modernize their IT and accomplish their missions.

The Federal Supply Chain at a Glance

What is a software supply chain attack?

Software code can be compromised through cyber attacks, insider threats or other close access activities at any phase of the supply chain to infect an unsuspecting customer.



Source: Director of National Intelligence (DNI)

"The supply chain threat is real."

William Evanina, Director of the National Counterintelligence and Security Center (NCSC), Office of the DNI, in 2018

$575 billion

represents the federal government's supply chain and acquisition functions that it hopes to modernize through regular engagement among supply chain management and acquisition experts.

$49 million

was in the supply chain management defense working capital fund in 2019.

2.2 million

people were affected by the CCleaner malware attack on a supply chain in 2017. Malware is malicious software created to damage computers and their related systems.

Jan. 1, 2021

is the date when the Defense Department (DoD) must formalize standards for supply chain and operational security and create requirements for microelectronics.

DoD traditionally had three acquisition pillars: Cost, schedule and performance. It added security as the fourth in 2018.

9 supply chain threat groups

including counterfeit parts and insider threats, were identified by CISA in 2019.

~300 impacts

across 10 risk archetypes — or fundamental categories — were identified by the DoD-directed Interagency Task Force regarding the manufacturing and defense industrial base in 2018.

21 countries

were identified by the Government Accountability Office (GAO) as the potential source of laptop memory supplier facilities in 2018. These supply chains can be long, complex and globally distributed, making the supply chain hard to track.

Possible Manufacturing Locations of Typical Network Components

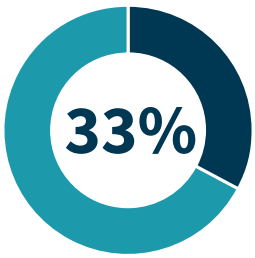
Component	Possible manufacturing locations
Workstations	United States, Israel, Spain, China, Malaysia, Singapore, United Kingdom
Notebook Computers	United States, Israel, Spain, China, Malaysia, Singapore, United Kingdom
Routing and switching	United States, India, Belgium, Canada, China, Germany, Israel, Japan, Netherlands, Poland, United Kingdom
Fiber optic cabling	China, Malaysia, Vietnam, Japan, Thailand
Servers	Brazil, Canada, United States, India, Japan, France, Germany, United Kingdom, Israel, Singapore
Printers	Japan, United States, Germany, France, Netherlands, Taiwan, China, Malaysia, Thailand, Vietnam, Phillippines

"There is a lot of active conversation across all agencies when it comes to supply chain."

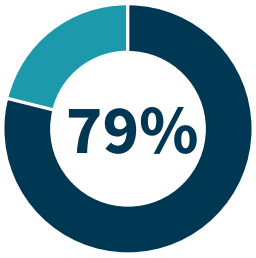
Dana Deasy, Chief Information Officer (CIO), DoD, in 2018

1990

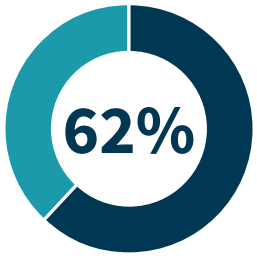
was when GAO added DoD supply chain management to its High-Risk List



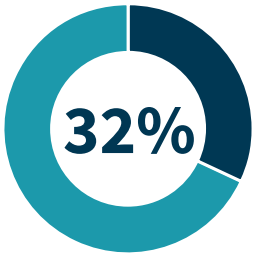
33% of IT professionals saw supply chain attacks as a concern in their organization in 2018.



79% of IT professionals believed that software supply chain attacks could become one of the biggest threats in the next three years.



62% of IT professionals said their IT leaders sometimes overlook software supply chain cybersecurity when deciding on their budgets.



32% of IT professionals' organizations vetted all their suppliers in 2017.

The Current State of the Federal Supply Chain – and the Case For Urgency

As IT supply chains grow more complicated, they also become more vulnerable. Much like a physical chain has physical links, IT supply chains contain interrelated parts that can become prey for bad actors.

Consequently, visibility into their entire IT supply chains can help agencies manage and mitigate security risks. ICT and services are crucial, and agencies blind to the dangers facing both categories are more susceptible to harm.

THE CASE FOR URGENCY

With supply chains, the devil's in the details. Consider smartphones — popular devices that contain hardware, software and multiple applications. For agencies trying to protect their communications technology and services supply chains, each category opens vulnerabilities.

Recall the federal government's recent concerns about Huawei and ZTE Corp., two Chinese technology companies that supply telecommunications equipment. The former also sells consumer electronics such as smartphones.

In November 2019, the Federal Communications Commission (FCC) barred companies from using its Universal Service Fund (USF) to purchase equipment and services from companies that threaten U.S. national security. USF provides billions of dollars in subsidies to companies to construct wireless services nationwide. FCC's decision to designate Huawei and ZTE as potential national security risks means businesses can't get these funds if they purchase equipment or services from either company. It also forces businesses that use Huawei or ZTE products and services to replace them before obtaining future USF money.

Supply chains challenge agencies at every level. In terms of hardware, smartphones contain multiple components such as computer chips, cameras and speakers. Although Huawei may be responsible for only some of those parts, agencies can't risk relying on it to make their smartphones. If they do, they become vulnerable to security risks, including data tampering, malware and spying.

"Both Huawei and ZTE have close ties to the Chinese government and military apparatus and are subject to Chinese laws requiring them to assist with espionage, a threat recognized by other federal agencies and the governments of other nations," FCC said in a press release about its ban targeting both organizations. "The public funds in the FCC's USF, which subsidizes U.S. broadband deployment and service through four separate programs, must not endanger national security through the purchase of equipment from companies posing a national security risk."

Unfortunately, a lack of visibility presents agencies with a harder challenge than ever in 2020. How do agencies get a grip on their supply chains before possible pitfalls such as Huawei and ZTE emerge? The answer is visibility into their full supply chains. From start to end, supply chains feature scores of parts, the producers who make them and the processes that keep them secure. Understanding every link in the chain can assist agencies with reducing the number of gaps in their defenses.

THE THREAT OF POOR SUPPLY CHAIN VISIBILITY

The ongoing drama over Huawei's and ZTE's influence on the federal communications technology supply chain demonstrates why visibility into such relationships matters.

For the federal government, the slightest misstep in a supply chain could present grave economic and national security consequences for the U.S. Huawei and ZTE are textbook examples of this dilemma: As Chinese companies, both are closely tied to China's government. As a U.S. rival, China can't be allowed to gain many advantages over the other nation.

FCC's decision to restrict how U.S. businesses partner with Huawei and ZTE shows the ripple effect that supply chain disruptions can generate. According to FCC, any damage to the federal communications supply chain could spread beyond technology.

"Modern communications networks are an integral component of the U.S. economy, enabling the voice, data, and Internet connectivity that fuels all other critical industry sectors — including our transportation system, electrical grid, financial markets and emergency services," FCC said in a statement about its constraints on Huawei and ZTE. "But these networks are vulnerable to various forms of surveillance and attack that can lead to denial of service, and loss of integrity and confidentiality of network services."

Supply chain turmoil can also hinder other valuable government actions such as IT modernization. FCC suggested that problems with the federal communications supply chain could hurt progress toward 5G, the fifth-generation wireless technology used in digital cellular networks that is widely considered the next level in communications.

"As the United States upgrades its networks to the next generation of wireless technologies — 5G — the risk that secret 'backdoors' in our communication networks will enable a hostile foreign power to engage in espionage, inject malware, or steal Americans' data becomes even greater," according to FCC's statement.

In its September 2019 report about supply chain threats, CISA broadly recommended the following steps for raising awareness of the likely perils in a supply chain:

- Sharing information among private-sector businesses, agencies and other public institutions about a supply chain's issues.
- Identifying, monitoring and developing prevention and response plans for all potential supply chain threats.
- Understanding which manufacturers and contract bidding partners present the least risk to a supply chain.
- Incentivizing partners to purchase products and services from the original equipment manager or authorized resellers.
- Mapping the lifecycle of products and services from start to finish so that a supply chain's weaknesses are noticeable.

Jointly, these maneuvers can help ensure agency leaders keep their eyes open for supply chain lapses.

THE 5G CONTROVERSY AND SUPPLY CHAINS

Concerns about supply chain cybersecurity have become a mainstream issue in part because of the advent of 5G broadband wireless networking.

5G is expected to bring a quantum leap in speed and capacity, enabling the development of new applications and services. Potential use cases include applications related to autonomous vehicles, video surveillance and telemedicine.

Two of the primary suppliers of 5G equipment are Huawei and ZTE, however, which has raised concerns about the security of the 5G environment.

In response to those concerns, the NDAA for Fiscal Year 2019, passed in August 2018, included a provision specifically prohibiting the federal government from buying certain telecommunications equipment or services from Huawei, ZTE and other Chinese companies.

In May 2019, President Trump issued an executive order giving the Commerce Department the authority to ban transactions involving information or communications technology designed, developed, manufactured or supplied by companies under the purview of a foreign adversary.

But how would the use of foreign-made equipment pose a threat to the 5G environment?

At a May 2019 Senate hearing, Christopher Krebs, Director of DHS's CISA component, identified two broad areas of concern:

- Data on 5G networks will flow through interconnected cellular towers, small cells and mobile devices that may provide malicious actors additional vectors to intercept, manipulate or destroy critical data.
- Malicious actors could also introduce device vulnerabilities into the 5G supply chain to compromise unsecured wireless systems and exfiltrate critical infrastructure data.

Concerns about cyber-related supply chain security are not new. For example, in October 2012, the National Institute of Standards and Technology (NIST) published Interagency Report 7622, "National Supply Chain Risk Management Practices for Federal Information Security."

"Federal departments and agencies currently have neither a consistent nor comprehensive way of understanding the often opaque processes and practices used to create and deliver the hardware and software products and services that it procures," the report states. This lack of understanding "increases the challenges associated with managing the risk of exploitation."

Huawei and ZTE were not the first foreign companies to be targeted by the federal government. In 2017, the government prohibited agencies from doing business with Kaspersky Lab, an antivirus firm, because of questions about its ties with Russia's government.

But concerns about 5G have triggered a much broader push to understand and address supply chain fears, in large part because the stakes are so much higher, threatening both economic and national security interests.

"Our adversaries have been developing and using advanced cyber capabilities in attempts to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democratic institutions," Krebs told the Senate.

Efforts to Improve Supply Chain Security

For years, federal, state and local officials have hoped for the best when managing the risk to their supply chains. Although security has always been a factor for these officials, they've grown accustomed to dealing with supply chain weaknesses as part of their jobs. This fresh federal interest is helping every corner of government strengthen their supply chains before refocusing on modernization.

DRIVEN FROM THE TOP: TRUMP'S EXECUTIVE ORDER

Illustrating the importance of strong supply chains, President Trump directed federal power in May 2019 toward repairing any flaws in America's communications and IT chains.

Trump's executive order appeared during a roiling trade war between the U.S. and China. Although aimed at communications and IT products and services, its implications quickly reached far beyond both fields. Trump's order doesn't name any countries or companies, but it made clear that the U.S. would no longer tolerate competitors' taking advantage of its supply chains.

"Foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people," he said.

The situation is "a national emergency" that presents "an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States," Trump added.

Because of the order, agencies nationwide can no longer purchase any communications or IT products or services that endanger U.S. national security.

Additionally, Trump's measure details several steps for eliminating the frailties in the federal communications and IT supply chains.

1. The measure charges the DNI with assessing every risk presented by the products or services from both chains within 40 days of Trump's order.

2. It tasks DHS with evaluating how reliant critical infrastructure organizations and service providers are on possibly risky hardware, software and services within 80 days.

3. It orders Commerce to publish procedures and regulations for reviewing relevant transactions within 150 days.

Additionally, the directive establishes a new normal for federal supply chains. Going forward, a coalition of government leaders including the Attorney General and the Commerce Secretary would determine which potential deals could raise red flags about national security. By working in concert, these changes aim to gradually shrink the number of holes in the federal ITC supply chains.

In November 2019, Commerce built on Trump's order by proposing rules for how it would gauge potential supply chain risks. Commerce Secretary Wilbur Ross said the department would practice a case-by-case approach to weighing possible threats and that any assessment would also include intelligence from DHS and DNI before a final decision is made.

Recently, the national intelligence community has repeatedly voiced fears that foreign spies are trying to infiltrate U.S. supply chains. Over time, Trump's order could reduce the number of prying eyes on these valuable systems.

RSA

Resilient in Times of Disruption

Build a resilient foundation to keep your business running

Learn More

INDUSTRY SPOTLIGHT

Seeing the Risks in Your Supply Chains

An interview with Rob Carey, Vice President/General Manager, Global Public Sector Solutions, and Dan Carayiannis, Archer Government Public Sector Director, RSA

When it comes to government supply chains, agencies can't properly defend what they can't see. As their networks of third-party vendors and IT components expand, agencies must reassess how they identify, manage and overcome supply chain risks.

Supply chains are the systems that move products or services from suppliers to customers, and they are only growing more complicated in today's hyper-connected world. Each supply chain contains activities, information, organizations, people, technologies, and resources that are vital to government operations. Consequently, supply chains are a top priority for agencies to understand, put controls in place, monitor, and help defend. Agencies that fail to understand their supply chain risks may spend significant energy, money and time addressing disruptions to their missions.

To learn how agencies can better monitor their supply chains, GovLoop spoke with Rob Carey, Vice President/ General Manager, Global Public Sector Solutions, and Dan Carayiannis, Archer Government Public Sector Director, at RSA, a cybersecurity and digital risk management solutions provider. They shared three tips for agencies to see supply chains risks more clearly.

1. Develop a risk-based view of supply chains

According to Carayiannis, supply chains create two major concerns for agencies. First, agencies must understand where vulnerabilities and risks exist among their contractors and subcontractors. Second, agencies must understand the technology components contractors leverage to support their organization's mission.

"Your risk domain has increased significantly," Carayiannis said of agencies adding contractors, components or both. "You need to account and plan for it. You must assess risk, manage findings and have recovery processes in place not only for yourself, but your contractors as well."

2. Assemble your supply chain security toolbox

Carey said that many agencies struggle to understand which vendors they contract with, what components they provide, and which manufacturers make them. According to Carey, tools that provide real-time information about these factors can boost agencies' supply chain security.

"The world for cyber professionals is getting more complex, but the right tools will help simplify things," he said.

RSA's Archer platform is one example of a tool that can help agencies quickly assemble information about their supply chains. In turn, this data helps agency leaders make smarter decisions about supply chain management.

3. Move to continuous monitoring

Continuous monitoring can help keep supply chains secure. It is a process that can make supply chain management more mature, robust and thoughtful. Continuous monitoring involves building risk profiles of a supply chain's main vendors and monitoring them for danger in real-time. Subsequently, agencies understand the threats and risks they face across their supply chains' ecosystem.

Tools such as RSA's Archer platform can assist agencies with recognizing, responding to and tracking risk remediation initiatives across their supply chain to include contractors and subcontractors as well as technologies.

"A hyperconnected world demands that the supply chain be examined, and that supply chain risk management be part of the language of the CIO and CISO so that they can continue to do their jobs," Carey said.

SUPPLY CHAINS: THE PATH FORWARD

Two agencies' efforts show how the federal government continues to make progress on shoring up its supply chains. Following their example, agencies can not only survive risks to their supply chains but thrive despite them.

Up first is CISA. Nestled within DHS, CISA aims to improve cybersecurity across all segments of government. CISA also coordinates cybersecurity programs with state agencies, and it improves the federal government's hacking defenses. Subsequently, CISA's mission neatly aligns with protecting the federal government's ICT supply chains.

Following Trump's executive order, CISA identified about 190 threats troubling agencies in a September 2019 report. It covers four elements of supply chain risk management: Information sharing, qualified bidder and manufacturer lists, procurement policy, and threat evaluation. The report also describes threats such as counterfeit parts that frequently trouble agencies.

In December 2018, CISA released an infographic detailing the six places vulnerabilities could infiltrate the ICT supply chains. They are:

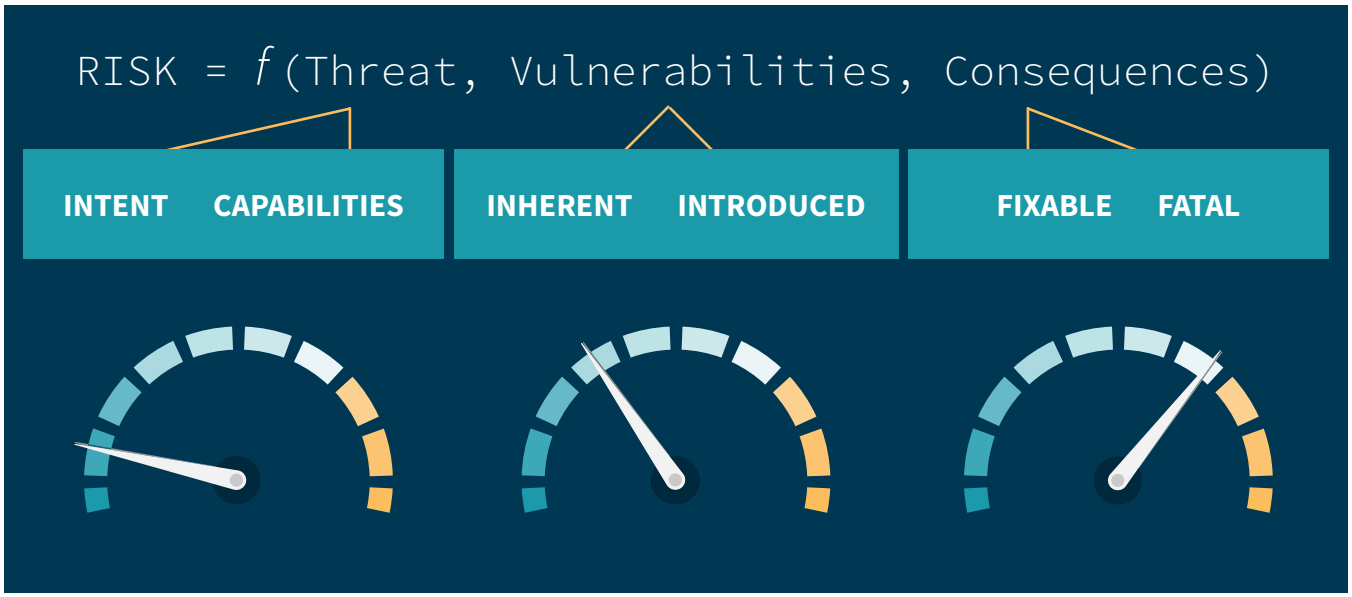
- **Design** — The design process for the components that make up technology such as smartphones.
- **Development and Production** — Processes such as assembly and manufacturing that physically create these tools.
- **Distribution** — The transportation routes that components take between the various production facilities involved in constructing these tools.
- **Acquisition and Deployment** — The procurement and installation processes for these tools.
- **Maintenance** — The process of monitoring, maintaining and upgrading these tools.
- **Disposal** — The process of disposing of or eliminating the components that comprise these tools.

In addition to CISA, NIST has been a longstanding resource for agencies struggling with their supply chains. In 2008, NIST launched its Cyber Supply Chain Risk Management (C-SCRM) program to help the public and private sectors improve how they manage risks associated with their global supply chains.

NIST now recommends five key practices for managing the risks involved with cyber supply chains. They are:

1. **Foundational Practices** — Establishing healthy cybersecurity and supply chain practices as the basis of an effective risk management program.
2. **Organization-Wide Effort** — Including all of an agency's organizational, mission and business process, and information system personnel on risk management.
3. **Risk Management** — Understanding the decisions and processes involved with acquiring, developing and delivering a supply chain's products and services.
4. **Evaluating Threats and Vulnerabilities** — Comprehending the types of threats and vulnerabilities that threaten agencies, and the appropriate responses to each.
5. **Identifying Critical Systems** — Deciding which components and systems will have the greatest effect on an agency if they're compromised can help agencies better defend them.

Collectively, CISA and NIST are shedding light on what agencies can do to keep their supply chains safe.



Source: NCSC

A RISK-BASED APPROACH TO SUPPLY CHAIN SECURITY

Agencies rely on globally sourced commercial technologies every day to power critical services and systems. But ensuring continuous security of those technologies is a never-ending battle.

Although agencies can't control the sophistication and frequency of attacks against their systems, they can take steps to improve their defensive posture. One way is through strong risk management, which includes assessing and evaluating alternatives to address risks – security, financial and otherwise.

In the past, risk management was viewed as a balancing act of cost, schedule and performance.

"But the risk landscape is constantly changing, which demands that the evaluation and management of those risks adjust accordingly," according to NCSC, which leads the U.S. government's counterintelligence and security activities. "Security is such an instance."

In its supply chain risk management framework, NCSC explains that "security must be added as a 4th pillar of the risk equation with equal emphasis to Cost, Schedule [and] Performance."

The government has neither the resources nor the capacity to detect and respond to every IT risk equally. And it can't eliminate all risks while still enabling employees to access what they need to do their jobs. So, what should agencies do?

Using the framework as guidance, we've highlighted some key points to keep in mind. For starters, your agency must understand its threats, vulnerabilities and consequences.

Threat: Understanding an adversary's intentions and capabilities is vital. The key is to use the latest threat information to determine if specific and credible evidence suggests adversaries might be targeting an item or service.

Vulnerabilities: Adversaries can be successful only if systems, processes and services are vulnerable to attacks. Vulnerabilities are weaknesses that are either inherent to the system or have been introduced into it by an outside agent.

Consequence: The consequences of the risk must be considered. If the threat is realized and the system is attacked and/or compromised, is the outcome fixable or fatal? What is the overall impact to employees, customers, the mission and the government as a whole?

Assessing these areas isn't a one-time event. But once agencies have a solid foundation for tracking, measuring and evaluating the threats, vulnerabilities and consequences they face, then they can determine dangers and develop a solid risk management program.

FORESCOUT®

The Leader in Device Visibility and Control

Gain Device Visibility and Control

Across Your Extended Enterprise

Campus

IoT

Data Center

Cloud

OT

Security at First Sight™

www.Forescout.com

INDUSTRY SPOTLIGHT

Supply Chain Risk Management Isn't Just About the Supply Chain

An interview with Katherine Gronberg, Vice President for Government Affairs, Forescout Technologies

Concerns over the risk to federal networks from supply chain threats have led to a slew of new government measures over the past two years aimed at mitigating this risk.

These include the Cybersecurity Maturity Model Certification (CMMC), which prescribes specific cybersecurity standards for suppliers to the DoD. The federal government has also banned its agencies and suppliers from using products that have been deemed extremely risky. But, according to Katherine Gronberg, Vice President for Government Affairs at Forescout Technologies, government IT users must also bear responsibility for implementing the proper policies and controls so that supply chain risk that is unknown or unavoidable can be mitigated after deployment.

Gronberg shared three ways federal agencies can leverage Forescout to mitigate risks to hardware and software deployed to federal networks.

1. Continuously monitor device behavior

NIST recommends agencies have continuous and comprehensive awareness of the IT assets coming and going from the network. "Monitoring all devices while they're connected gives agencies the ability to identify anomalous device behavior and take action," Gronberg said. This is the overarching objective of two major federal cybersecurity programs, the Continuous Diagnostics and Mitigation (CDM) program for civilian agencies and the Comply to Connect (C2C) program for DoD."

"The government should implement policies that incentivize or require better security practices from suppliers. But it also needs to ensure agencies can remain secure even when their devices are not."

2. Segment devices into like groups

Network segmentation isolates devices and device communications into separate areas of the network to limit their access. According to Gronberg, "Proper network segmentation can prevent attackers from communicating to a compromised device, and it can block the unauthorized exfiltration of data."

Network segmentation as a control category is moving toward dynamic network segmentation, in which segmentation policies are enforced automatically and in real time to separate traffic for any user or device. "Forescout profiles devices in real time as they connect and disconnect from the network, enabling the application of segmentation rules based on this real-time data," Gronberg explained.

3. Aspire to Zero Trust

Zero trust is an end-state where devices and users can only access network resources if they have demonstrated the requisite level of security and authorization. It requires continuous assessment of these devices and users while connected. The Forescout platform enables customers to identify all the devices connected to their networks and provides them real-time, in-depth information around these devices. It then allows customers to use this information to take actions and build policies that improve overall security posture. "Forescout believes all assets should be distrusted, regardless of where they're made or who makes them," Gronberg said.

Federal agencies today are better equipped to implement these best practices because of the Forescout capabilities they have received through the CDM and C2C programs. "The federal government has realized that managing supply chain risk is not just about vetting or prohibiting suppliers and products. It is also about helping agencies use them safely," Gronberg said. "CDM and C2C are doing this."

DHS Task Force Takes Point on Supply Chain Security

In late 2018, DHS established the ICT Supply Chain Risk Management (SCRM) Task Force to support public and private efforts to improve supply chain security. GovLoop spoke with Bob Kolasky, Director of the NRMC at DHS's CISA, to learn more about the task force's evolving work.

The interview below has been lightly edited for brevity and clarity.

GOVLOOP: What is the task force's guiding mission?

KOLASKY: The task force brings industry and government together to discuss ways to build capabilities and address issues that will help us better mitigate risk to the nation's ICT supply chain. That's going to take coordinated and integrated activity across government, with industry's involvement. We find that having industry at the table as part of the task force leads to the implied force multipliers and pushing out risk management practices. We also get better insight into what effective government action might be.

How do you define risk-informed decision-making when it comes to the ICT supply chain?

We're primarily talking about making risk-informed decisions on where you get your underlying hardware and software to operate systems, and the confidence you have in the integrity, function and availability of that hardware and software to support the operations of information communications technology.

Risk comes from companies that may be under the influence of foreign laws that require certain things to be shared with foreign governments. Risk comes from places that don't have good security practices in place, even if it's not for malevolent reasons. The more confidence you have that the equipment you're buying and the companies you're buying the equipment from are top-notch, the less risk you're taking.

We want to continue to build processes to allow and encourage companies and government agencies that want to do the right thing and don't want to take risks to have the tools and information to do that.

What do you say to agencies that might feel overwhelmed by the number of threats?

It's a tough thing. We do try to organize it around nine general threat categories. But at a certain level, you start [to ask] which ones are more important?

We wanted to have a full view of where experts thought the threats would come from. What we are going to try to do with that in future iterations is boil it down to things that are a little easier to consume for people who don't have significant supply chain risk management programs. But I think you must start with realizing that these are the things that could be out there.

I think, intuitively, a lot of folks will be able to look at the threats out there and say, "These are the ones that are probably most applicable to my particular supply chain," and start to neck it down to risks of concern and what they can do about those risks. That's some of the work the task force will be doing in year two.

How do you see threat information sharing in government evolving?

The threat information you're sharing about supply chain risks has a lot to do with the factors we were talking about earlier. [For example,] are you concerned about a business that is in your supply chain? That's different than cyber threat information sharing, which is about indicators and IP addresses and can be automated. This is more contextual.

We, in DHS, concluded that the risk of Kaspersky Lab software on government systems was too high, and we wanted to share that information — why we made those decisions — as broadly as [we could]. We can do certain things with federal authorities to restrict use in federal systems, but we want to encourage state and local systems, industry systems, to look at the information we have and make decisions like that.

We learned some lessons in our work with Kaspersky and similar work that helped in the first year of the task force. But one of the things that the working group members identified was that there is private-to-private information-sharing gaps. A big IT company or comms player could decide not to do business with somebody. They're not necessarily sharing that information with other players in the ecosystem, because they're concerned about their ability to do so. We think we can make some recommendations around policy shifts, statutory shifts, that maybe would encourage more sharing so there's less risk in sharing information.

How do you think supply chain risk management needs to evolve for the future?

Supply chain risk management is a discipline that is becoming more and more important because of the risk environment. It's not something that can be solved. It's something that we're going to continue to build out. Across the federal space and in industry, there needs to be more investment in understanding supply chains and building out the capability to reduce risk. That's what we're focused on in the task force — not just what we can get done in two years, but how we can continue to set the conditions for enhanced supply chain security over the next decade-plus.

qmulos®

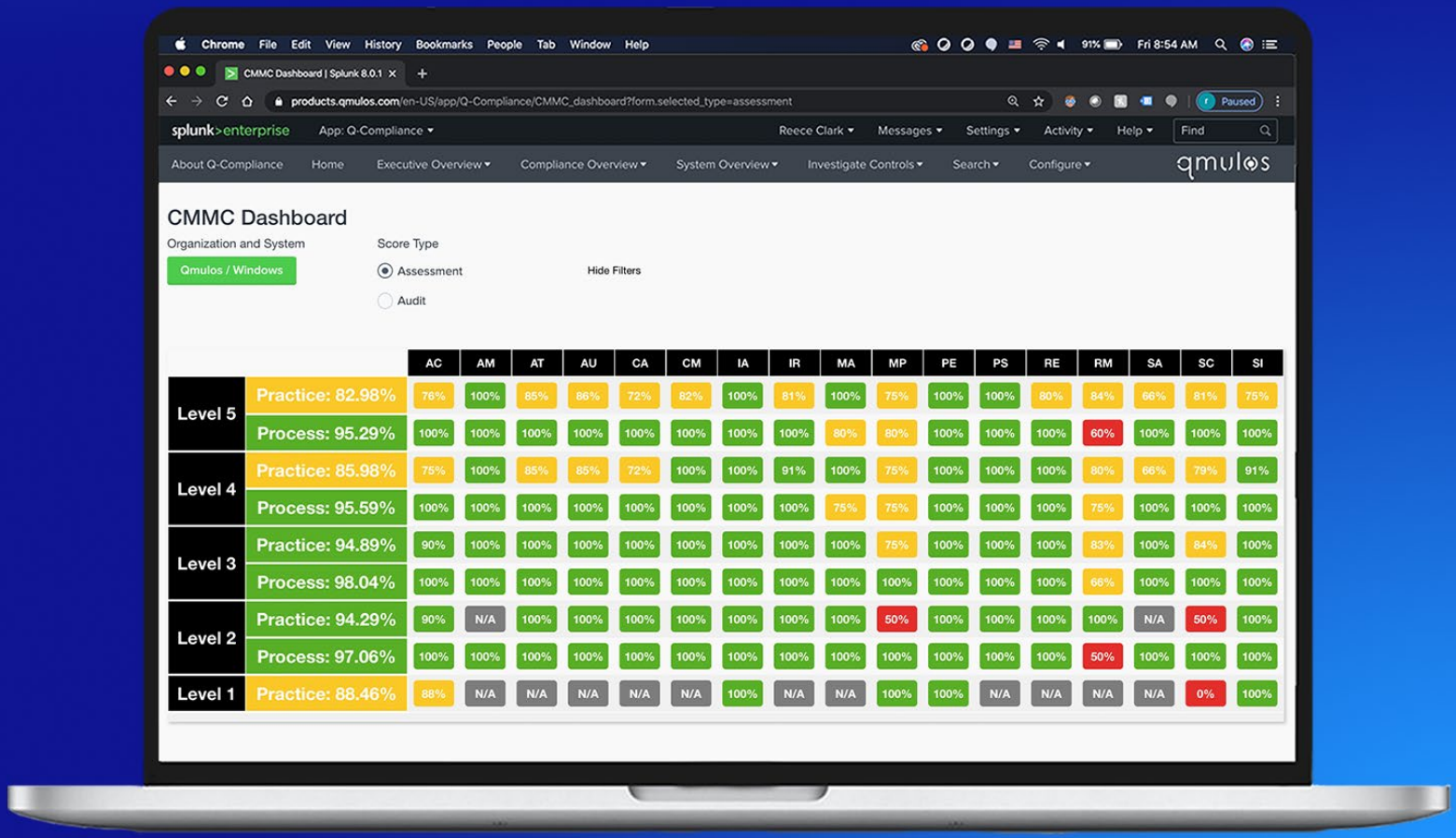
Automated Cyber Compliance Monitoring.

Out with the old. In with the new.

Real time continuous monitoring is the future. Qmulos offers an all-in-one solution to optimize operational security for ANY size enterprise, ANY environment, ANY framework, ANY control, ANY data source.

Learn more at qmulos.com/q-compliance

To request a demo email sales@qmulos.com



		AC	AM	AT	AU	CA	CM	IA	IR	MA	MP	PE	PS	RE	RM	SA	SC	SI
Level 5	Practice: 82.98%	76%	100%	85%	86%	72%	82%	100%	81%	100%	75%	100%	100%	80%	84%	66%	81%	75%
	Process: 95.29%	100%	100%	100%	100%	100%	100%	100%	100%	80%	80%	100%	100%	100%	60%	100%	100%	100%
Level 4	Practice: 85.98%	75%	100%	85%	85%	72%	100%	100%	91%	100%	75%	100%	100%	100%	80%	66%	79%	91%
	Process: 95.59%	100%	100%	100%	100%	100%	100%	100%	100%	75%	75%	100%	100%	100%	75%	100%	100%	100%
Level 3	Practice: 94.89%	90%	100%	100%	100%	100%	100%	100%	100%	100%	75%	100%	100%	100%	83%	100%	84%	100%
	Process: 98.04%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	66%	100%	100%	100%
Level 2	Practice: 94.29%	90%	N/A	100%	100%	100%	100%	100%	100%	100%	50%	100%	100%	100%	100%	N/A	50%	100%
	Process: 97.06%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	50%	100%	100%	100%
Level 1	Practice: 88.46%	88%	N/A	N/A	N/A	N/A	N/A	100%	N/A	N/A	100%	100%	N/A	N/A	N/A	N/A	0%	100%

INDUSTRY SPOTLIGHT

How to Make CMMC Deliver Value

An interview with Tieu Luu, Chief Product Officer, Qmulos

In January 2020, DoD released the final draft of the Cybersecurity Maturity Model Certification (CMMC). CMMC measures the maturity of a contractor's cybersecurity processes and practices across the IT environment. The first release of CMMC focuses on protecting data that is categorized as controlled but unclassified information (CUI).

DoD plans to incorporate CMMC audits into the procurement process – so there's a lot at stake for defense contractors. But given its complexity, how can organizations make CMMC compliance manageable? To learn more, GovLoop spoke with Tieu Luu, Chief Product Officer at Qmulos, which provides solutions for monitoring cybersecurity compliance. He recommended three key principles that should guide compliance efforts.

1. Don't see CMMC as a stand-alone challenge

Any organization that works with DoD is likely already implementing various security standards and requirements, including numerous standards defined by NIST.

Many agencies mandate NIST's Cybersecurity Framework (CSF), the Risk Management Framework, the security controls defined by NIST Special Publication (SP) 800-53, and NIST SP 800-171, which identifies controls for protecting controlled unclassified information in non-government systems.

If organizations try to tackle each mandate individually, they can get buried in compliance work. Instead, they should create workflows for collecting compliance data across the board, then filter by requirements – an "assess once, report against many [frameworks]" approach.

"If you're treating each mandate separately in a piecemeal fashion, then it's just inefficient," Luu said.

2. Make real-time visibility a priority

Cybersecurity is dynamic and evolving. The mix of end-users, applications and services is changing in response to shifting customer requirements. The threat environment evolves as well, as new adversaries emerge, and older adversaries adopt new tactics.

Because of that, compliance assessments often are out of date just days, hours or minutes after they are completed, Luu said. "To have confidence in what you're reporting, you need to base that on real-time data that you're collecting about your networks, devices and even your end-users," he said.

The need for real-time intelligence is best met by building on a scalable big data platform – one that is capable of ingesting, visualizing and analyzing data from a wide range of tools, said Luu.

3. Use many tools but one platform

Many factors go into determining compliance with CMMC, depending on the level of protection required. The challenge is integrating all those factors to provide a comprehensive view of compliance.

For example, among the 17 capability domains are access controls, identification and authentication, physical protection, and system and communications-level protection. Organizations likely are using multiple tools to implement controls and track compliance across each of those areas.

To make sense of it all, they need an underlying platform such as Qmulos' Q-Compliance that simplifies that environment: Integrating the tools, normalizing the data for analysis and aligning specific security controls with the CMMC's requirements. Automation is also essential, both in terms of assessing compliance and identifying and remediating potential risks, Luu said.

Why Better Acquisition Practices Are Key to Supply Chain Security

One of the best ways to reduce risk to the IT supply chain is to address that risk during the acquisition process. For example, in developing the Air Force's Second Generation IT multiple-award contract, the General Services Administration (GSA) incorporated supply chain risk management requirements. To learn more about the intersection of acquisition and supply chain security, GovLoop spoke with William Zielinski, Assistant Commissioner, Information Technology Category, at GSA.

The interview below has been lightly edited for brevity and clarity.

GOVLOOP: What are the risks that need to be addressed as part of the acquisition process?

ZIELINSKI: From an acquisition perspective, we have a lot of variability in how agencies are buying their technical capabilities. Because of an increased threat environment, there's greater likelihood that we could suffer. It's much more difficult to respond when there's such variability in how we're acquiring our business capabilities.

So, what you're seeing is a lot of growing recognition that as an overall government, we are better served by looking at the threats that are present in the environment and moving some measures earlier in the value chain. In other words, rather than allowing agencies to buy whatever they want and then figure out what the risks are, we're better served if we approach the market as an overall government whole and [move] some of those protections and risk buy-downs at the beginning of the phase, the acquisition phase.

How do you broadly explain to someone what those threats are?

If you're looking at it from a couple broad perspectives, the first one I would say is from a business continuity perspective. As you acquire the capabilities that you need to run your business, there's threatened risk involved with something happening to one of those products or services that would disrupt the operation of your essential functions as an agency. In that case, we're not necessarily looking at it from an attack perspective.

Bucket two falls more into national security, where there is a purposeful actor moving to disrupt some activity. They're either trying to obtain critical information or they're looking to do denial-of-service attacks or ransom attacks with intent of some gain. And they could be carrying out those attacks either by something that was specifically introduced in the supply chain or by having knowledge of where vulnerabilities already exist in the things that you're buying.

How can agencies address increased risks without hampering their acquisition processes?

The first thing I'd say is knowing and understanding there is risk in the environment. You can't boil the ocean and try to solve everything all at one point in time, so taking a risk-based approach is a starting point.

First, what that means is that agencies need to assess and understand the threats that are within the delivery of their business. Second, their assessment should be informed by standard guidance and best practices. For example, NIST organizes cybersecurity activity at the highest level to

identify, protect, detect, respond and recover. Through these functions, agencies can manage their cybersecurity risk by having good risk management frameworks. If an agency starts there, by knowing and understanding where those risks are outside of an acquisition, and if they do this as a normal course of business, they have a good foundation.

Third, the risk and assessment that they have performed should also be informed by their own business continuity plans. In other words, if they're looking at their critical business and mission-essential functions as a lens, then they have a sense of the capabilities they need and how to buy those things today. By using that NIST framework and organizing the threats and risks, they have a good set of information by which to shape their acquisition.

So, what I'm saying here is this: What I just described should be part of normal business planning. In that way, when agencies are moving to acquire or buy some capability, it should not hinder their efficiency or effectiveness.

How can technology itself improve supply chain security efforts?

For one, [regarding] the sundry pieces of legislation that have come through around supply chain risk, we actually started a Robomod pilot for prohibited products. It is a process to identify and remove prohibited products and compatible products from across the offerings that we have, from different contracts and from our buying platform. In this instance, it was started around the Kaspersky ban, ZTE [and] Huawei. It goes across the thousands of different products that are associated with those prohibited product areas, and we can do the work of locating, isolating and moving forward in the removal of those products in mere minutes, as opposed to what would take humans weeks to be able to crawl through and search for those things. We're finding great results in being able to do that.

What's the take-away for agencies looking to better manage supply chain risk?

While each agency through the SECURE Technology Act is being asked to take on some new functions or duties, rather than each agency trying to reinvent the wheel or go this alone, I would urge them to reach out to folks like us in GSA, where we've been thinking through this from a governmentwide perspective. There are opportunities for us to help further their efforts above and beyond and to connect them with others who have also been looking for ways to address their supply chain risk issues.

Reduce Cybersecurity Risks in Your Supply Chain

Discover unknown risks with continuous, technically verified monitoring across the entire Internet.

Place zero trust in self-attested compliance, and don't let point-in-time audits become compliance theater. With Expanse, you get a comprehensive asset inventory program to continuously discover and monitor risks associated with digital assets across your attack surface — including the global attack surface of your strategic suppliers. Visit us at Expanse.co to learn how we can enhance your Supply Chain Risk Management program.

EXPANSE

INDUSTRY SPOTLIGHT

Internet Assets Are "Unwitting Insiders": A Challenge To Traditional Supply Chain Risk Management (SCRM) Programs

An interview with Dr. Matt Kraning, Co-Founder and CTO, Expanse

Traditionally, IT and acquisition leaders have thought about their cyberattack surface in terms of physical IT assets, such as laptops, servers and networks. But there's an important class of assets that don't fit into that traditional management framework – such as IP addresses, domain names and cloud instances – that introduce risks into the cyber supply chain.

GovLoop spoke with Dr. Matt Kraning, Co-Founder and CTO of Expanse, who leads the implementation of cyber SCRM projects with the DoD and Defense Industrial Base primes like Lockheed Martin. He discussed four key steps to enhancing the maturity of SCRM programs through digital asset inventory.

1. Scale best practices in attack surface reduction

Leading organizations that successfully limit their cyberattack surface share two characteristics: A comprehensive asset inventory program that includes the inventory of digital and ephemeral assets including IP addresses, domains, certificates, and cloud instances; and a comprehensive program to dynamically and continuously discover new parts of their attack surface anywhere they may appear on the Internet, including on assets previously unknown to the organization.

2. Place zero trust in self-attested compliance, and don't let point-in-time audits become "compliance theater"

A security policy is only as good as its enforcement: Place zero trust in self-attestation. Moreover, depending on the threat environment faced by an enterprise, point-in-time audits may be insufficient relative to continuous validation of asset management practices. Every employee is now a de facto systems administrator who can spin up risky Internet assets in minutes. That means the entire Risk Management Framework (RMF), which is a cyclical model to be repeated as necessary, fails at Step 1 if a current, accurate and complete asset inventory is not maintained to manage risk relating to internet-exposed assets.

3. How continuous should "continuous monitoring" be?

The problem with continuous monitoring as implemented in most environments is that monitoring is too infrequent, and only known assets are monitored. Successful continuous monitoring requires comprehensive asset management. As written in NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Systems and Organizations, "More accurate system component inventories support improved effectiveness of other security domains such as patch management and vulnerability management."

By necessity, a mature SCRM program facing an acute threat environment must apply a daily-or-better refresh rate to point-in-time audits of dynamic internet assets.

4. Scale Internet asset management across your cloud assets and key suppliers

DoD's Cybersecurity Maturity Model Certification (CMMC) program has delivered baseline maturity levels focused on the protection of information hosted on premises. There remains, however, a critical capability gap to baseline risks relating to "weak links" like cloud hosted assets and key suppliers, often the principal vectors of attack.

Just as agencies should develop a comprehensive inventory of their own Internet assets, Kraning said, they need to overlay continuous, risk-based SCRM initiatives to address the extended attack surface presented by key suppliers. The costs are no longer prohibitive.

Best Practices in Supply Chain Risk Management

The world of supply chains is complicated, filled with moving parts and unpredictable factors. And, as supply chains expand globally, these threats will continue to ramp up, especially with the introduction of software and technology that may be hard to test.

Preparing for and responding to modern supply chain threats require agencies to coordinate and institute best practices. Below are actions that NCSC's Supply Chain Directorate recommends.

1. Establish Internal Policies and Processes

To prepare for the spectrum of supply chain threats, an organization first needs a strategy. Working across teams and affected parties, agencies need to craft internal policies and processes that implement SCRM. Then, agencies should carve out roles and responsibilities for team members and identify maturity levels for programs to reach. The resulting plan should address preparedness and responsiveness, clearly describing an escalation process and delegating decision-making authority. Finally, the plan should cement SCRM as a part of an annual risk assessment.

2. Identify a Supply Chain Risk Manager

Supply chain risk management needs a voice of authority. Someone from the executive team should be designated the supply chain risk manager. From there, a team should follow suit, taking part in SCRM executive board meetings. This multi-disciplinary team can then design the specific policies and plans described in the first practice.

3. Enhance Contract Language for Supply Chain Security

The difficult part of supply chain is that it isn't a two-way street. With all sorts of moving parts, in fact, agencies need to get the details from vendors. Built into contracts, requirements should include metrics for supply chain security along with cost, schedule and performance. Agencies should also negotiate the right to audit important suppliers' supply chains and verify their compliance with terms, laws and standards. These practices protect the supply chain's integrity and make it easier to remediate the damage from breaches.

4. Train and Educate Employees

Employees throughout an organization should understand what's in the supply chain process. Managers should be aware of escalation plans and have general knowledge of policies and protocol. SCRM professionals particularly — those in the fields of cybersecurity and acquisition — need to know how SCRM fits into their other day-to-day roles. And as the field continues to evolve, it would be ideal for employees to seek out training, which should be reviewed and updated annually.

5. Share Information

There are supply chain risk management communities that leaders and employees should be encouraged to join. These communities, as well as conferences and other online information-sharing groups, can help employees and leaders keep up with the latest news in their field.

6. Identify Critical Assets and Services

Consider assets' risks and importance to agencies. In some cases, a tradeoff of high risk for minimal importance might lead agencies to look for other solutions. On the other hand, sometimes high-risk supply chains may be unavoidable for key assets, and then agencies have the responsibility to protect the supply chains. The board should develop a way to determine risk tolerance and tradeoffs and create contingency plans in case the supply chain is disrupted or breached for these assets.

7. Conduct SCRM Assessments

Agencies can't protect what they don't know. By auditing the SCRM process, agencies can track supply chains, check results and compare their security postures to those of other organizations. These processes should be regular and random to guarantee their reliability, and they should yield areas for improvement in SCRM.

8. Exercise Due Diligence on Suppliers

There's only one way to know which suppliers can be trusted. Agencies need to research suppliers before completing transactions, as well as consider security right alongside price, schedule and quality. Going through authorized sellers is a way to ensure sellers are trustworthy, and agencies then can limit the amount of work they have to do alone. To truly get the best all-around contracts that will practice good SCRM, agencies need to reframe the acquisition mindset from lowest cost to best value. Defining a rubric for "best value," agencies can then train employees, and agencies should reward those who excel in meeting the criteria.

9. Perform Damage Containment and Strengthen Defenses

When the supply chain is compromised, agencies need to be ready. Following an incident response plan, agencies should be prepared to analyze what happened and contain the damage. Effective response means that agencies will have visibility into their supply chain and can implement best practices from other agencies that were in similar situations.

FOR MORE INFORMATION ABOUT BEST PRACTICES:

See the full NCSC list of recommendations.

Review the FBI's best practices here.

Check out a resource provided by NIST.

IronNet

BECAUSE THE SUM IS GREATER ...

Secure your digital supply chain with IronNet Collective Defense.

Collective Defense is the new approach to cybersecurity that:

- Enables companies, including supply chain stakeholders, to work together within and across sectors to defend against targeted cyber threats in real time
- Facilitates threat knowledge sharing across the the Collective Defense ecosystem for faster response to threats detected by network behavior analysis

"Cyber attackers are acting together in sophisticated ways … why wouldn't we defend together if we have the technology? By collaborating and sharing threat information at network speed, all companies in a Collective Defense ecosystem can have advanced notice of incoming threats — and defend more proactively."

— General (Ret) Keith Alexander, former Commander U.S. Cyber Command and current Co-CEO and Founder of IronNet Cybersecurity

Discover more in the Collective Defense eBook or visit IronNet.com

INDUSTRY SPOTLIGHT

Securing Supply Chains With Cyber Collective Defense

An interview with Jamil Jaffer, Senior Vice President for Strategy, Partnerships & Corporate Development, IronNet Cybersecurity

Supply chain complexity is rising, and the public and private sectors are stronger together. The resulting approach is called cyber collective defense, and it's changing how businesses and the federal government protect their supply chains.

To learn more, GovLoop spoke with Jamil Jaffer, Senior Vice President for Strategy, Partnerships & Corporate Development at IronNet Cybersecurity, a global cybersecurity leader who is delivering the first-ever collective defense platform to secure enterprises, industries and governments.

1. Understand your agency's threat landscape

Agencies that map out their entire supply chains are more prepared for responding to a cyberthreat landscape that changes daily. According to Jaffer, agencies are in an unusual predicament when it comes to supply chain security. "The federal government relies on contracting with small businesses and large corporations," he said. "Each of these has their own cybersecurity vulnerabilities and risks."

To defend themselves, Jaffer recommends that agencies ensure their suppliers identify and monitor all the data, processes and systems involved in their supply chains to defend them as a single ecosystem. "Rather than relying on entities in the supply chain to defend against the most capable threat actors, including Russia, China, Iran and North Korea, agencies should have their suppliers share critical threat information in real-time to defend the entire supply chain as a whole," said Jaffer.

2. Create shared situational awareness and collaboration

Legacy information sharing processes are designed to react after a cyberattack is under way or once a threat has been identified. According to Jaffer, in the modern environment, agencies and their suppliers need to get ahead of threats and identify them faster. "Attackers are moving rapidly," he said. "If our threat sharing and cyber collaboration isn't happening in real-time, and if we aren't focused on the behaviors that indicate preparations for an attack, we'll continue to fall far behind the attackers."

Cyber collective defense addresses these problems by having multiple agencies, along with their suppliers, work collectively to defend against an attack. For instance, agency security operations centers (SOC) can share threat information with their suppliers and other agencies to triage threats, enabling more flexible, rapid defense. "By creating a common operating picture across multiple vendors and agencies, each individual agency can identify threats that might otherwise have gone unnoticed in a single environment," said Jaffer. "And, perhaps most importantly, they can leverage each other's resources," Jaffer said of cooperating agencies and suppliers. "They can work together in identifying and defending across each other's entire threat landscape. In addition, this approach helps solve the problem of limited staff resources and cyber tools that all of our agencies face."

3. Focus on resilience and recovery

Unfortunately, supply chains are so complex that security incidents are often a question of if, not when. According to Jaffer, agencies that quickly share information and resources are better equipped to withstand and recover from such attacks. "It's important to have the right systems in place when attackers come," he said.

What do the right systems look like? According to Jaffer, supply chains thrive when agencies have a cyber collective defense platform that enables the identification of breaches faster and allows quick reaction times for defenders. "Being able to identify an attacker faster and take action against them is critical to limiting the impact of an attack and to restoring services," said Jaffer. Platforms such as IronNet's combine collaboration with rapid threat-sharing. The outcome is agencies that can read and react to any situation involving their supply chains at a moment's notice. "We provide a cybersecurity umbrella over our private-sector partners and federal agencies," Jaffer said. "They can collaborate in real-time to divide and conquer when it comes to stopping threats."

What's Next For Supply Chains?

When presidents act, agencies notice. Trump's recent executive order on securing the federal government's ITC supply chains promises to ripple across every category of agency.

Starting with federal agencies, Trump's measure ties national security to every product and service inside the ICT supply chains. But the order doesn't stop making waves there; going forward, state and local agencies will have their own roles to play in supply chain security. With many of these chains boasting thousands of links worldwide, government unity will be crucial for preventing threats from harming them.

The private sector also has a newfound responsibility to secure supply chains after Trump's move. Gone are the days when businesses could partner with any component provider they wanted. Trump's order puts pressure on companies to proceed with caution on supply chain relationships that could hurt national security. And it pushes them to work more closely with every type of agency. In today's increasingly connected world, only information sharing between governments and industries can ensure that no supply chain remains partially obscured.

Supply chains threats aren't disappearing any time soon. For cyber criminals, supply chain vulnerabilities are too valuable an opportunity for profit to pass up. For hostile foreign governments, these same weaknesses could give them a decisive economic, military or political edge over the U.S. With such high stakes, agencies can't afford to neglect their supply chain vigilance.

Trump's policies mark a valuable first step toward securing America's supply chains. Should future administrations follow suit, the products and services citizens enjoy will come from supply chains that are increasingly safe and sound.

ABOUT CARAHSOFT

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®. As a top-performing GSA Schedule and SEWP contract holder, Carahsoft serves as the Master Government Aggregator™ for many of its best-of-breed technology vendors, supporting an extensive ecosystem of manufacturers, value-added resellers, system integrators and consulting partners committed to helping government agencies select and implement the best solution at the best possible value.

Visit www.carahsoft.com, follow @Carahsoft, or email sales@carahsoft.com for more information.

THANK YOU

Thank you to Carahsoft, Expanse, Forescout, IronNet, Qmulos, and RSA for their support of this valuable resource for public sector professionals.

ABOUT GOVLOOP

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector. For more information about this report, please reach out to info@govloop.com.

AUTHORS

Mark Hensch, Senior Staff Writer
Nicole Blake Johnson, Managing Editor
John Monroe, Director of Content
Isaac Constans, Senior Staff Writer
Pearl Kim, Staff Writer

DESIGNER

Kaitlyn Baker, Creative Manager

Strengthening the Security of Government Supply Chains

Carahsoft's solutions providers are committed to mitigating risks to agencies' supply chains.

CYBERARK
dun & bradstreet
EXIGER
EXPANSE
FICO
FIREEYE
FORESCOUT
.govini
IronNet
McAfee
MICRO FOCUS Government Solutions
MOCANA
okta
paloalto NETWORKS
qmulos
RSA
SailPoint
SAP
servicenow
sonatype
splunk>
SWORD GRC
SYNOPSYS
+ableau

Carahsoft's Supply Chain solutions are available through its reseller partners on a variety of contracts including Carahsoft's GSA Schedule 70, SEWP V, NASPO ValuePoint, and numerous state and local contracts.

To learn more, contact us at (888) 662-2724 or SCRM@carahsoft.com

carahsoft

Carahsoft's Supply Chain solutions are available through its reseller partners on a variety of contracts including Carahsoft's GSA Schedule 70, SEWP V, NASPO ValuePoint, and numerous state and local contracts.

Learn more at carahsoft.com/innovation.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop