FEDERAL NEWS NETWORK

EXPERT EDITION

Get ready to take on software supply chain risk management

Insights from

- CISA
- OMB
- State Department

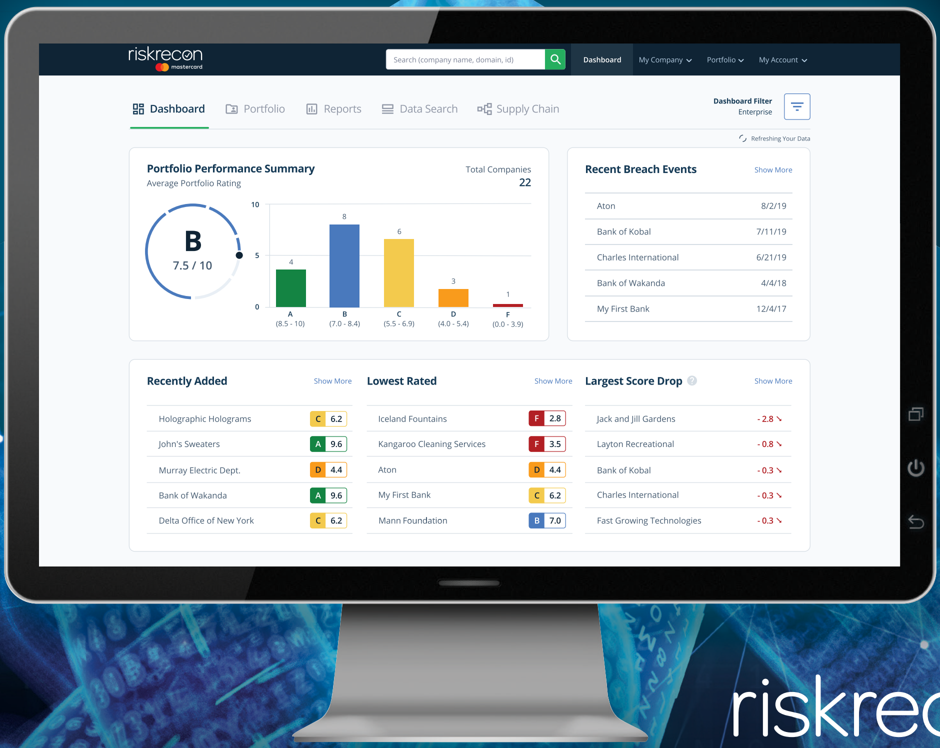
BROUGHT TO YOU BY riskrecon mastercard

Secure Your Digital Supply Chain

As a cybersecurity professional, making agile decisions with limited information is no easy task. Fortunately, RiskRecon lets you analyze the security performance of your digital supply chain.

During our 30-day free trial, you can get a detailed view of the risks of up to 50 companies in your provider ecosystem, allowing you to make more informed decisions based on risk data.

Start your free trial at www.riskrecon.com/know-your-portfolio



Portfolio Performance Summary

Average Portfolio Rating

Total Companies 22

Recent Breach Events Show More

Aton	8/2/19
Bank of Kobal	7/11/19
Charles International	6/21/19
Bank of Wakanda	4/4/18
My First Bank	12/4/17

Recently Added Show More

Holographic Holograms	C	6.2
John's Sweaters	A	9.6
Murray Electric Dept.	D	4.4
Bank of Wakanda	A	9.6
Delta Office of New York	C	6.2

Lowest Rated Show More

Iceland Fountains	F	2.8
Kangaroo Cleaning Services	F	3.5
Aton	D	4.4
My First Bank	C	6.2
Mann Foundation	B	7.0

Largest Score Drop Show More

Jack and Jill Gardens	- 2.8 ↘
Layton Recreational	- 0.8 ↘
Bank of Kobal	- 0.3 ↘
Charles International	- 0.3 ↘
Fast Growing Technologies	- 0.3 ↘

riskrecon
mastercard

TABLE OF CONTENTS

Do you have the visibility you need into your software supply chains?

Ultimately, agencies will need to use a mix of tools and research to ensure they have a complete picture of the supply chains for all government-owned and run software.

It really comes down to a fairly basic question, which the Cybersecurity and Infrastructure Security Agency's Bob Costello put succinctly: "You can often use code from all over, but are you really checking that code and ensuring that it doesn't have malicious hooks into it, and that it's what you expect it to be?"

That's the question at the heart of current governmentwide efforts to establish supply chain risk management for federal software. All agencies must, over the next two years, hit a series of SCRM milestones outlined by the Office of Management and Budget in its fifth and final memo related to the president's executive order on improving cybersecurity. OMB issued the memo in September 2022.

"These requirements apply to agencies' use of software developed after the effective date of this memorandum, as well as agencies' use of existing software that is modified by major version changes," explained Federal Chief Information Security Officer Chris DeRusha.

Determining the supply chain details of software bought, used and developed by the government requires gaining a depth of knowledge more expansive than the vast majority of agencies previously tracked about the who, what, where, when, why and how of their software.

"Without a tool, it's hard to really verify beyond the self-attestation" that the government will ask vendors to provide, pointed out the State Department's Zetra Batiste.

In this ebook, we get a good understanding of the task ahead from CISA, OMB and State about what agencies must do to develop supply chain risk management programs and what it will take to gain the deep visibility necessary to verify the security of software used across the government.

Vanessa Roberts
Editor, Custom Content
Federal News Network

Understanding the basics of software supply chain risk management

BY ALEXANDRA LOHR

As federal agencies and contractors come to grips with the burden of protecting their software supply chain, understanding who had a hand in the development of software products has taken on increasing importance. It comes down to pedigree. Where did your software come from? Was it domestic or international? Who had a hand in developing it?

"For lack of a better term, company profiling: Is there foreign ownership? Are there concerns with how this company's operating model is, when you get deeper than that? What are their software development practices? Is it within the United States? Is it offshore? If it's offshore, what countries is software development being done under?" said Bob Costello, chief information officer for the Cybersecurity and Infrastructure Security Agency, in an interview for ***Federal Monthly Insights - Supply Chain Risk Management***.

> "When you start having discussions about software development practices, are they following a good methodology? Do they have security kind of baked in throughout their development and process?
>
> — Bob Costello, Chief Information Security Officer, CISA

Beyond understanding provenance, Costello said it's essential to take a look at software development practices. "You can often use code from all over, but are you really checking that code and ensuring that it doesn't have malicious hooks into it, and that it's what you expect it to be?"

President Joe Biden released Executive Order 14028 on improving cybersecurity in May 2021. It directed the National Institute of Standards and Technology to issue guidance "identifying practices that enhance the security of the software supply chain." The order also directed the Office of Management and Budget to require agencies to comply with the National Institute of Standards and Technology's supply chain risk management (SCRM) guidelines when procuring software.

SCRM must dig into the how of software development

As agencies work toward compliance with the executive order, they have to look at a number of issues, Costello said in an interview with Federal News Network's Jason Miller. If their prime contractors have documented compliance, they also need to check compliance of subcontractors down the line in the software development process.

“When you start having discussions about software development practices, are they following a good methodology? Do they have security kind of baked in throughout their development and process?” he said. “Those are things that we want to look at because those are the things that we want to be doing on our site when we’re doing government development.”

Part of the process of providing evidence of software supply chain security is self-attestation. Any agency procuring software needs to have self-attestation from its software developers stating that development followed NIST’s SCRM standards for secure procedures. According to NIST guidelines, attestation should focus more on ongoing practices than on specific pieces of software design.

Costello views self-attestation more as a jumping off point for SCRM than as what will eventually become mature security practices across the government.

“We want to get to a better place than just self-attestation. But that won’t always be required or possible. We should really be looking at what is the risk,” he said, and then added that people generally are “not good at gauging the true risk of things. And it’s really hard on the government side. But in some cases, there could be data that is low risk, it’s exposed, and we should consider that maybe those companies that are handling that don’t need quite the level of vetting that we may want for a company handling or designing software for national security systems or dependent systems or others. There could be varying levels based on what the product is doing.”

SCRM applies across the development ecosystem, not just to primes

As supply chain risk management matures, finding the root source of software needs to become part of the formula. Finding those sources creates a challenge for primary contractors who are supplying software products to agencies, Costello said. Contractors may be relying on one or more subcontractors to provide part of a software package. While the prime may have a good sense of the security of its product, tracking and ensuring that subcontractors have been equally rigorous can be more difficult.

“Oftentimes, our contracts don’t have a stipulation that only the prime can do the work. … Like I always tell my primes, ‘Well, I just view it all as a prime. I don’t care that it’s company XYZ.’ There will have to be an expectation that they are doing due diligence,” Costello said.

> “
>
> Like I always tell my primes, ‘Well, I just view it all as a prime. I don’t care that it’s company XYZ.’ There will have to be an expectation that they are doing due diligence.
>
> — CISA’s Bob Costello

Listen to the full discussion between Federal News Network’s Jason Miller and CISA’s Bob Costello on implementing supply chain risk management

State Department works toward SBOM adoption to improve SCRM practices

BY DAISY THORNTON

Software bills of material get a lot of attention as tools to help federal agencies improve their supply chain risk management. Although there's some disagreement over when agencies will start benefiting from SBOMs, many agencies are currently laying the foundation to start using them.

In fact, the State Department has created a working group to develop guidance and procedures on how to capture and store them.

"We're not there yet," said Zetra Batiste, enterprise chief information security officer for cybersecurity supply chain risk management (C-SCRM) at State's Bureau of Information Resource Management. "However, we do realize the need for ongoing collaboration with industry and government stakeholders to ensure that we're harmonizing that federal effort on automating and building a repository of SBOMs for reciprocity."

Often described as an ingredient list for software, SBOMs create transparency by detailing the various components in a piece of software and the dependencies between those components.

Agencies must address SBOM challenges

There are currently a number of challenges inherent in the use of SBOMs that need to be solved, Batiste said during ***Federal Monthly Insights – Supply Chain Risk Management***. For one thing, they need to be automatically generated and machine-readable. Developing the processes and formats for that aren't easy. Add on top of that a general lack of training and knowledge of how SBOMs work since they're a fairly new concept.

When they are used, a software development team has to stop what it's doing every time an SBOM reveals a vulnerability and mitigate that vulnerability, which takes time. And sometimes a vulnerability turns out to be a false positive. It's one reason the C-SCRM team is currently working on a solution to ingest SBOMs.

Until that happens, agencies have to work with self-attestations. State is also looking into options for

> Without a tool, it's hard to really verify beyond the self-attestation.
>
> —Zetra Batiste, Enterprise Chief Information Security Officer for Cybersecurity Supply Chain Risk Management, State Department

third-party tools to verify the accuracy of those self-attestations, but that will take time as well, she said.

"Without a tool, it's hard to really verify beyond the self-attestation," she said on the ***Federal Drive with Tom Temin***. "But I think it starts with forming that relationship with the developer, so that you understand you're forming that bond, that relationship, so that you understand his third-party vendors, etc. And you use processes too, such as assessments to validate where required, where you can."

State plans to continuously monitor for vulnerabilities

In the meantime, State is pursuing software that can continuously monitor for any vulnerabilities, Batiste said. Her team created an assessment process for risk, including examining a vendor's foreign relationships and potential threats to infrastructure that its software might pose. From there, the department makes a decision about whether to try to mitigate that risk or simply avoid using the software altogether.

Another thing State is focusing on is collaborating with the Cybersecurity and Infrastructure Security Agency and other cybersecurity working groups to promote information sharing about threats and vulnerabilities across agencies. Those groups are also working together on surmounting the barriers to SBOM adoption, she noted.

"Vulnerability that hits one eventually touches us all," Batiste said. "So the more we learn, the better we're able to collectively protect our infrastructure."

> "Vulnerability that hits one eventually touches us all. So the more we learn, the better we're able to collectively protect our infrastructure.
>
> — State's Zetra Batiste

Listen to the full discussion between The Federal Drive's Tom Temin and State's Zetra Batiste on adopting SBOMs to improve SCRM

With software memo out, OMB moves into cyber EO implementation phase

BY JASON MILLER

The Office of Management and Budget has outlined 17 initiatives for agencies to take in 2023 and 2024 to secure their software.

The focus of the initiatives, however, is solely on commercial software and not government-developed applications.

Chris DeRusha, federal chief information security officer, said OMB is starting with commercial off-the-shelf software and not agency-developed or government off-the-shelf software (GOTS).

“This memo is focused on an agency that purchases commercial third-party software. That’s regardless of if they customize that software after the purchase. That’s all in play here,” DeRusha said on ***Ask the CIO***. “We also do state explicitly in this memo that agencies are expected to be following these practices. We have and we will continue to do plenty to ensure that agencies are following secure development practices. That’s a core part of any good security program. It’s something that we definitely track at OMB and discuss a lot with the CISO Council.”

In the memo, OMB defines third-party commercial software to include firmware, operating systems, applications and application services such as those in the cloud, as well as products containing software.

“These requirements apply to agencies’ use of software developed after the effective date of this memorandum, as well as agencies’ use of existing software that is modified by major version changes (e.g., using a semantic versioning schema of Major.Minor.Patch, the software version number goes from 2.5 to 3.0) after the effective date of this memorandum,” the memo stated.

One of the first deadlines, to inventory all software, comes in December 2022. Agencies must also provide a separate inventory of applications deemed critical. OMB leaned on the National Institute of Standards and Technology’s definition of critical software from 2021.

> “
>
> We have and we will continue to do plenty to ensure that agencies are following secure development practices. That’s a core part of any good security program. It’s something that we definitely track at OMB and discuss a lot with the CISO Council.
>
> — Chris DeRusha, Federal Chief Information Security Officer, Office of Management and Budget

Moving into next phase of cyber EO

OMB's decision to start with commercial software carries with it the potential for both risk and reward. Software must be the enabler of agency mission success, DeRusha said. The use of commercial software, especially in the cloud, has grown at double-digit rates over the last decade.

The Alliance for Digital Innovation reported in 2019 that market research firm Deltek estimated federal spending on commercial software between 2018 and 2023 would account for about 11% of the more than $664 billion in total IT expenditures during that five-year period.

Of course, as more agencies moved to the cloud over the last two years, the security of those services have become more important.

OMB shifts cyber focus to implementation and measurement

The software memo was the fifth and final memo that the cyber EO directed OMB to issue.

DeRusha said OMB will therefore shift its focus to implementation mode in the coming months.

"We're working on getting good data and performance measurement metrics around the policies. You can expect moving forward to start to see public-facing metrics, showing how well we're doing based on everything that we set in place," he said. "We had to do that first. Then we are definitely going to start ensuring that we're telling the story with data. That'll take a little time. But that's coming."

OMB also is working on new Federal Acquisition Regulation rules to meet the requirements under Section 2 of the EO around sharing threat intelligence as well as Section 4, which is related to the software security memo.

> "
>
> We're working on getting good data and performance measurement metrics around the policies. You can expect moving forward to start to see public-facing metrics.
>
> – OMB's Chris DeRusha

"Those are going to be a big deal because that's really about getting contract clauses right and solid across all federal government agencies. That's a really big lift but also a really, really important one that will lift everybody up," DeRusha said. "There's just a lot of work attached to all this, but we do feel good that we've gotten through five really important memos and really instantiating clear guidance and direction about our priorities and where we need to head. We're excited about the implementation phase, and we're just staying busy and continuing the hard work."

Listen to the full discussion between Federal News Network's Jason Miller and OMB's Chris DeRusha on ensuring the security of COTS software bought by the government

Why it takes a fourth party to accomplish third-party software supply chain risk assessments

BY TOM TEMIN

Across the government, agency IT teams continue working to figure out how best to meet the demands of an executive order from May 2021.

EO 14028 on improving cybersecurity calls for the government to enhance software supply chain security. The operating principle behind the order might be obvious, if long neglected. Namely, that software as delivered to agencies consists of many parts and components, which means knowing the origin of all the pieces is critical to assessing and managing risks and threats. Some elements have been coded by a vendor's own staff, and some are open source.

That multiplicity of provenance is why the order calls for software bills of material (SBOMs). It also, at least in the short run, requires self-attestation by vendors about the reliability of their code and of the systems on which they developed the code. Therefore, a big challenge for federal buyers of software is visibility into their vendors' supply chains.

"What it really comes down to is gaining situational awareness of that software supply chain, and maybe that's sometimes easier said than done," offered John Ehret, vice president of strategy and risk for RiskRecon, a Mastercard company.

> In the security world, we have the idea of 'trust but verify.' When it comes to the software supply chain, we do an awful lot of trusting and not much verifying.
>
> — John Ehret, Vice President of Strategy and Risk, RiskRecon, a Mastercard Company

Software supply chain risks: Leap of faith

"In the security world, we have the idea of 'trust but verify.' I think when it comes to the software supply chain, we do an awful lot of trusting and not much verifying," he added.

It's a crucial issue because installing software in effect extends an agency's perimeter to the third parties in the supply chain of the installed application, Ehret said.

“If any one of those [suppliers] is the weak link, all the money we spent and the time and effort to secure that internal network that we cared so much about is really for naught,” he said.

An SBOM is a useful tool as far as it goes, but Ehret advises also implementing third-party risk management tools and techniques used commonly in the business world and adopting them to federal software supply chains. When doing so, he said, agency practitioners must keep in mind that third-party risk assessment in the commercial world focuses on financial and operational risk. In the federal world, agencies often have the added pressure of national security.

Still, “once you know what makes up that software, the different components of it and who those suppliers are, then you can start to take a look at those companies themselves and kind of gain a sense for what their hygiene looks like,” Ehret said.

Make sure risk assessments dive deep into the supply chain

He cautioned that third-party risk organizations tend to be small and lightly resourced, and it therefore might be difficult for them to take on government software supply chains, which can be extensive.

“That’s where different tools, and not just solely relying on the humans, really comes into play,” Ehret said.

Even before deploying tools though, it’s wise to take a risk management approach to assessing and prioritizing all the elements in the agency’s supply chain, he said. That way, the security team will be able to concentrate on the most critical applications first, Ehret advised.

> We asked third-party risk programs if they felt that self-attestation security questionnaires were accurate in depicting the effectiveness of controls in an organization. Only 34% said yes.
>
> — RiskRecon’s John Ehret

After that, the key is gaining visibility into the layers of secondary suppliers beyond the vendors from which the agency acquires software.

Self-attestation of security practices, as noted, is only a start, he said. Ehret cited a RiskRecon survey of clients that asked if they thought self-attestations by vendors were accurate in depicting the effectiveness of an organization’s controls.

“Only 34% said yes,” Ehret said.

So what can an agency do beyond that? He advised having a “Swiss army knife” of tools at the agency’s disposal.

For primes and subcontractors, the agency might ask for documentation of software coding practices, patch policies and disaster recovery plans. In some instances, such as cloud-provided software, the agency might be able to use a continuous monitoring tool to check its security, Ehret said.

Financial monitoring of suppliers, and of suppliers' suppliers, can also help in mitigating risk. It's important, Ehret explained, because financially distressed companies might cut back on their cyber or coding hygiene practices unbeknownst to developers or product users. Then, if a cyberattack occurs, they might not be able to respond to the degree needed, he said.

"Maybe that particular software supplier was kind of tenuous when it comes to their financial health," Ehret said. "So now you must start to wonder, because of this cyber event, are they going to actually go out of business? Then suddenly, we have a hole that we can't fill because it's a critical application."

That's why RiskRecon's deep assessment approach can fill an agency's monitoring needs several layers into a vendor supply chain, he said. RiskRecon often can identify and evaluate the potential risk of companies that agencies might not have the privileges or capability to monitor, Ehret said.

Listen to and watch the full discussion between The Federal Drive's Tom Temin and RiskRecon's John Ehret on gaining supply chain situational awareness