



Government intervention, the rise of the SBOM and the evolution of software supply chain security



Software Supply Chains in the Crosshairs

The past three years have witnessed exponential growth in software supply chain attacks. As Sonatype's 8th Annual State of the Software Supply Chain report revealed, such incidents have surged by 742% on average each year since 2019, with hackers increasingly viewing the software supply chain as an easy and lucrative target. SolarWinds, Log4j, and more recently MOVEit, have underscored the enormous impact vulnerabilities within the software supply chain can have and, as a result, are prompting government intervention on a global scale.

In the wake of SolarWinds, the US government led the global legislative charge by introducing the **Executive Order on Improving the Nation's Cybersecurity** (EO 14028) in May 2021, igniting the software supply chain security conversation and putting **Software Bill Of Materials** (SBOMs) front and center.

Then, following Log4j, the Biden administration set its sights on improving open source security with the **Securing Open Source Software Act**, followed by **2023's National Cybersecurity Strategy**. Crucially, the latter solicited Congress to begin developing legislation that will **allow the prosecution of companies** that introduce vulnerable software into the market.

Building on the policy established by EO 14028, the Executive Branch in the US is also utilizing its control over federal agency budgets (made possible by the Office of Management and Budget—OMB). The OMB establishes guidelines both for the procurement process (including SBOM requirements) and budgets of federal agencies looking to purchase software.

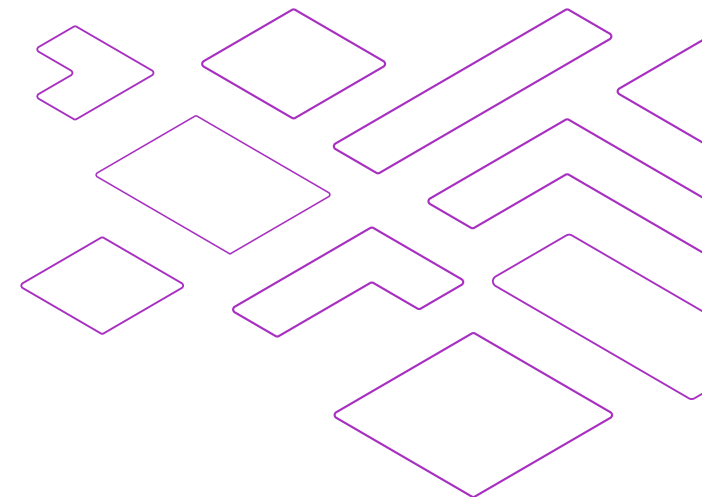
The current scope requires that agencies have all contractors self-attest to secure software development practices (based on NIST standards and best practices), with an option to require SBOMs. Taking this a step further, the OMB is tying these requirements to budget approval. Finally, as part of the **National Cybersecurity Strategy Implementation Plan**, Objective 3.5 focuses on leveraging federal procurement policy to improve accountability and grant the ability to leverage the False Claims Act to hold any contractor liable for falsely representing secure development steps they have attested to.

Software Supply Chain Security Incidents such as Log4j and SolarWinds, and arguably the US' regulatory response, also catalyzed other nations into action. In September 2022, the European Union announced its proposed **Cyber Resilience Act**, while in February 2023, the UK Government **published a Call for Views on Software**

Resilience and Security for Businesses and Organizations, both of which placed emphasis on SBOMs and wider supply chain security practices

But as more regulatory initiatives are put forward, how much are they impacting and improving software development and, ultimately, cybersecurity? Where is SBOM adoption, two years since the Biden administration issued its ground-breaking Executive Order mandating them? And how are companies adapting to this challenging threat landscape?

To examine this, we surveyed cybersecurity leaders at large enterprises (over £50 million/\$50 million annual revenue) across both the US and the UK to discover what's changed, how this tightening regulatory environment is being perceived, and the steps and missed opportunities to bolster software supply chain security.



Is Regulation Moving the Security Needle?

Despite cybersecurity policy being viewed as a headache by some, our findings show that the majority of business leaders consider it to be hugely influential (and needed) in driving the software security agenda forwards.

When asked which factors have most positively impacted their business' software security, cyber regulation was the top response, with 41% of the vote. Although other factors like increasing security team size and improving technology were not far behind. Figure 1 demonstrates a clear consensus regarding specific regulations, with the survey indicating that all the major policies listed are considered effective by the majority of respondents. This highlights the positive impact these regulations have had and also perfectly highlights how US regulation holds significant sway over UK cyber security policy.

This highlights the positive impact these regulations have had and also perfectly highlights how US regulation holds significant sway over UK cyber security policy.

Our findings show that opinion is pretty evenly split on which legislation is “most”

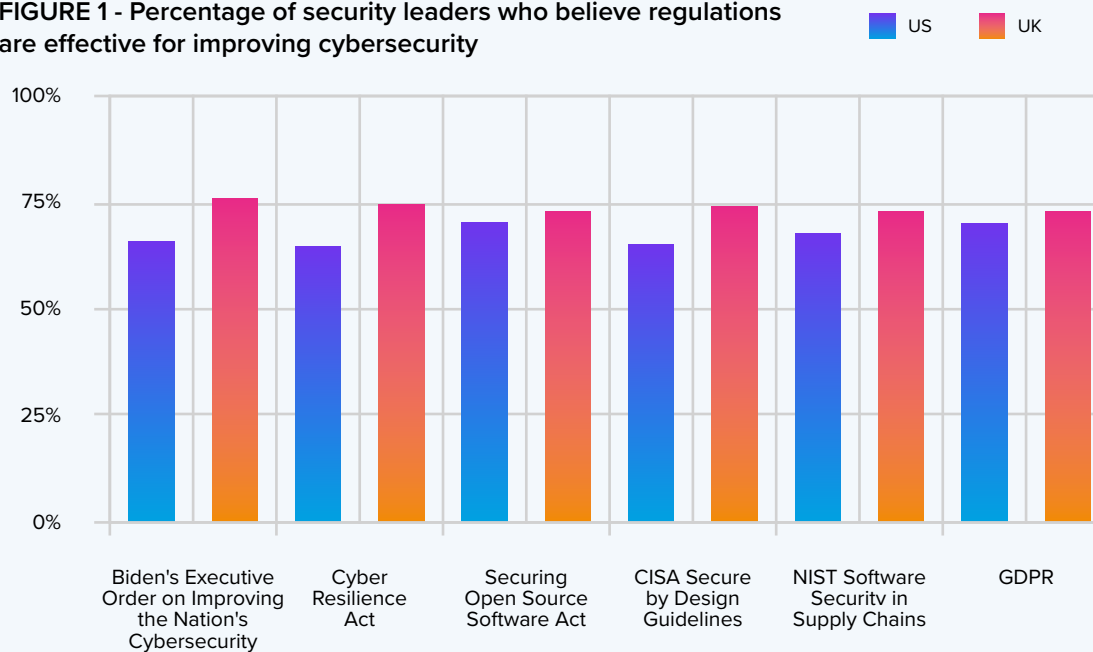
effective at improving security posture Figure 2. The Securing Open Source Software Act is marginally ahead, with almost a quarter of votes, and equal support from both US and UK leaders, hinting at increasing recognition of the critical need for improved open source hygiene.

Interestingly, the CISA Secure by Design Guidelines is considered far more influential by UK companies, while the NIST software security in supply chains regulation is preferred in the US - even though both

pieces of legislation come from the United States.

This could be due to the fact that despite the CISA guidelines originating from the US federal government, the approach was published in **partnership with several governments** including the UK's National Cyber Security Centre. This more global approach is encouraging to see and has been well-received by UK companies, according to our data.

FIGURE 1 - Percentage of security leaders who believe regulations are effective for improving cybersecurity



While our research found that security leaders believe regulation to be a net positive, the picture is less clear when it comes to how much regulation exists in total, with **44%** believing there is too much government intervention **Figure 3**.

However, it seems respondents are far more receptive to supply chain security guidance and regulation, given **76%** see it as positive, although again, we've observed some disparity between the US and the UK.

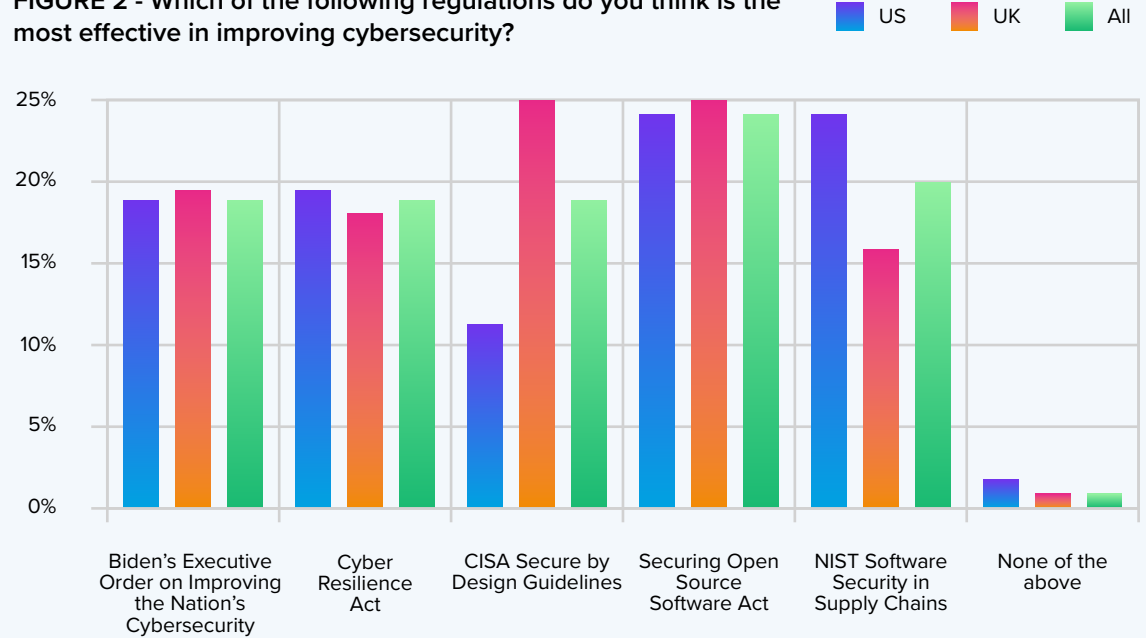
Despite **84%** of US IT leaders feeling positive about the supply chain regulation and guidance in their country, only **68%** feel the same in the UK. This is notable given the US has significantly more regulatory initiatives in place to address cybersecurity, indicating there may be an appetite for more, or perhaps more effective, regulation in the UK.

Although it's encouraging to witness regulations driving positive change and enhancing cybersecurity posture, effectively combating cyber threats requires a holistic approach involving not just government but the participation of C-Suite executives, developers and suppliers of software. Regulations can help establish a framework, provide guidelines, and set minimum standards for cybersecurity practices.

Application attacks and breaches frequently arise from vulnerabilities that are both easily exploited and easily remedied.

For optimal effectiveness, a more global

FIGURE 2 - Which of the following regulations do you think is the most effective in improving cybersecurity?

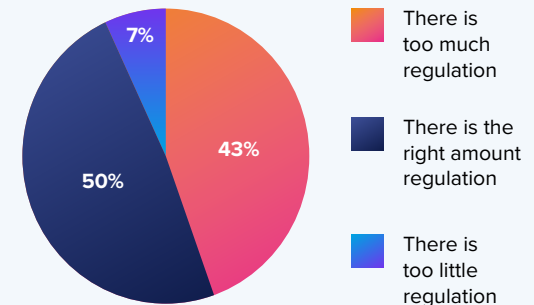


and collaborative approach is needed, along with the right tools and technology.

For optimal effectiveness, a more global and collaborative approach is needed, along with the right tools and technology.

While we'd like to believe companies are proactively prioritizing their cybersecurity measures in our software-dependent society, the regular occurrence of breaches in the news, even in the wake of more regulations, implies that governmental guidance is necessary to trigger true action.

FIGURE 3 - How do you feel about the amount of security guidance and regulation in your country?



The SBOM Explosion

Our findings also revealed that President Biden’s Executive Order on Improving the Nation’s Cybersecurity has fundamentally altered how companies are approaching software development.

Designed to enhance information sharing between the government and private sectors and promote the use of secure

software development practices, the order notably mandated that companies doing business with the US government must implement an SBOM. Like an ingredients list for software, **SBOMs** improve supply chain transparency and allow businesses to quickly identify and mitigate vulnerabilities. **But two years on from the landmark order, where are we now?**

Another **8%** have plans beyond this year, while only **1%** have yet to make plans at all. There is strong evidence to suggest that Biden’s EO had a significant influence on this, with **95%** of those companies implementing SBOMs doing so within the last two years, and **42%** of them specifically citing the order as their primary motive.

Other main drivers of adoption include improving cybersecurity posture, improving productivity, and keeping up with increasing cyber threats.

Our survey found that a huge **92%** of respondents either maintain an SBOM (**76%**) or plan to in the next year (**16%**).

FIGURE 4 - Do you maintain a software bill of materials (SBOM) for your applications?

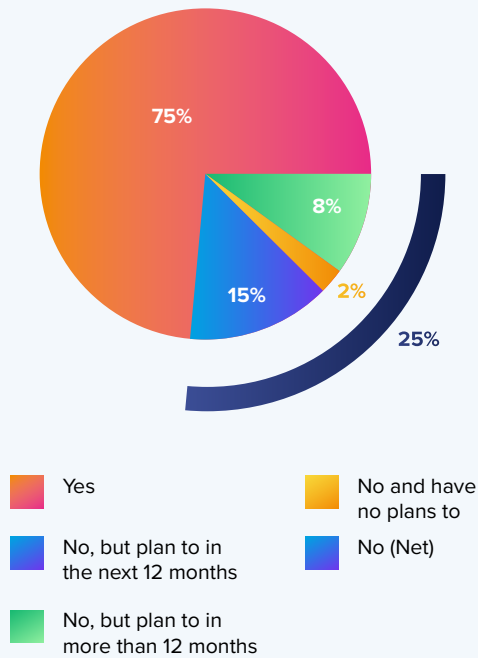
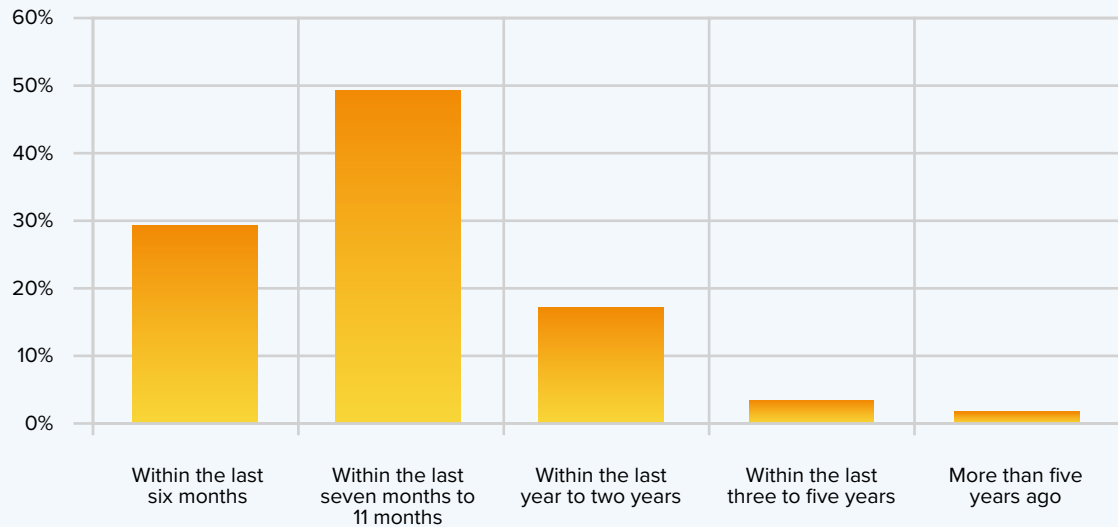


FIGURE 5 - If yes, when did maintaining SBOMs become common practice within your organization?



As SBOMs become widely implemented, companies that are slow to introduce them will find themselves at a major disadvantage. Not only will they not be able to identify and fix vulnerabilities significantly increasing the likelihood of attack they will be shut out of commercial opportunities if other governments and organizations follow the US' lead and stipulate they will only work with companies that maintain SBOMs.

And, given a huge **60%** of enterprises stated they require businesses they work with to maintain an SBOM, and a further **37%** stated they will do so in the future, it's clear that SBOMs are rapidly becoming a must for businesses in both the UK and US.

it's clear that SBOMs are rapidly becoming a must for businesses in both the UK and US

Our research also suggests that companies that have implemented SBOMs are updating them frequently, with over half (**53%**) updating their SBOMs multiple times a week. This is encouraging to see, as it's good practice to update SBOMs with each new software version release and in today's fast paced industry, companies are typically putting out several releases a week.

However, the best approach is to have automated, continuous monitoring of SBOMs to promptly address any new vulnerabilities or developments, ensuring 24/7 protection.

FIGURE 6 - If not, why have you decided not to implement SBOMs? (select all that apply)



Despite these positive signs, perceived barriers remain. Of the quarter of enterprises yet to implement SBOMs, cost and lack of knowledge of how to effectively implement them were cited as the main barriers, hinting that both further knowledge and resources may be needed to bolster supply chain security.

While further education around SBOMs is clearly necessary to fully close the gap, there are more **free resources** available to businesses than ever and the initial cost required to implement them pale in comparison to the impact of

potential breaches or loss of commercial opportunities from not having them in place. Effectively implementing SBOMs requires developing a detailed inventory of software components, automating SBOM generation, integration with the development pipeline, conducting vulnerability management, and enforcing policies.

By following this guidance, organizations can effectively leverage SBOMs to strengthen software security, improve risk management, and ensure better resilience against cyber threats. To learn more, see **[Sonatype's SBOM Quick Start guide](#)**.

Beyond the SBOM

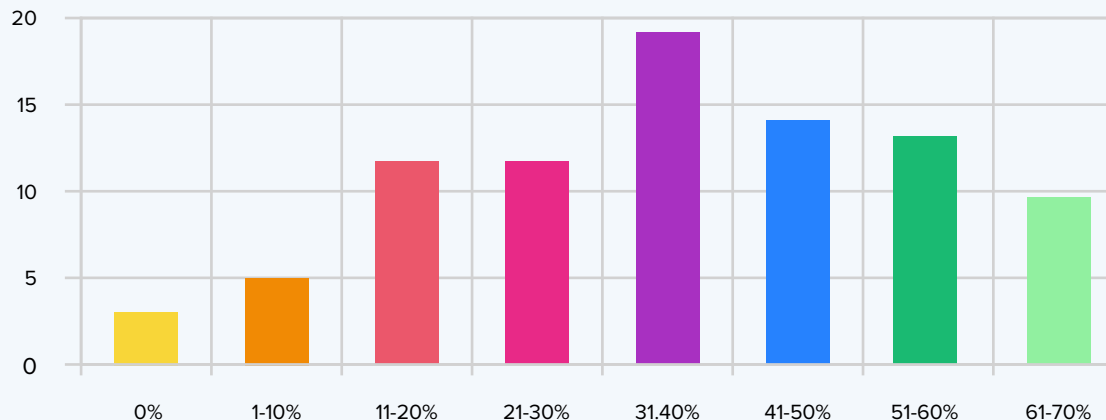
Although clear momentum is building for SBOMs and businesses and governments are rightly recognizing the vital role they play in improving software supply chain security they are just one step in a broader strategy. SBOMs are great at identifying the problem, but companies need to do more to actually solve it by actively tracking and fixing vulnerabilities.

But the scale and complexity of modern software supply chains, and the fact that around **90%** of modern code bases are open source means traditional manual methods of finding and fixing vulnerabilities are not up to the task. This is why Software Composition Analysis (SCA) tools have risen in prominence they automate visibility into open source software to help with risk management, security improvements and license compliance.

This enables businesses to manage and secure the use of open-source and third party software components in their applications through component analysis, vulnerability detection, and continuous monitoring, significantly reducing the risk of breaches.

But, going beyond the SBOM naturally requires additional buy in from stakeholders and prioritization of supply chain security. It's therefore good to see that some **33%** of large enterprises are now dedicating over

FIGURE 7 - What percentage of your cyber security budget is dedicated to software supply chain security?



half of their security budget to software supply chain security (rising to **40%** when looking at UK companies).

Even more encouraging, however, is the fact that **80%** have had their supply chain security budget increased compared to last year, as businesses recognize the critical need to bolster their supply chain security as threats surge.

Regarding where this budget should be invested, SCA tools should be a top priority for businesses that don't already have them in place. Visibility into the software supply chain and its components isn't enough organizations need

protection from the beginning. This means empowering developers with the tools and intelligence (including AI) they need to build and maintain secure, quality code.

With **54%** of our respondents claiming they spend between 6-20 hours each month fixing vulnerabilities in their software, solutions that help automate this process or block malicious code at the source can not only improve overall security posture, but can save resource strapped teams precious time.

SCA tools should be a top priority for businesses

Adopting smarter upgrade schedules can also deliver time and money savings remaining on safe versions and delaying upgrades until necessary can save **around two weeks per development team per year**.

For example, Sonatype's platform includes capabilities that automatically block malicious open source components at the door (Sonatype Repository Firewall) and provides comprehensive remediation guidance for developers to select the safest components. It can also quickly identify and replace vulnerable components present in applications (Sonatype Lifecycle).

Instead of taking days (or maybe longer for larger projects) to remediate transitive dependency risk with an SBOM, developers can do it in minutes. These efficiencies allow developers more time to focus on innovation and enable enterprises to scale. The benefit of going beyond the SBOM saves more than time, it saves the future of your organization.

In addition, Sonatype offers free tools and resources to help businesses start securing their supply chains right away. Our **Launchpad** is a library of information to help teams better understand software supply chain management. The **Open Source Vulnerability Scanner** is a free online tool that can scan an application and provides not only a complete Software Bill of Materials but creates a list of any security vulnerabilities, license and quality

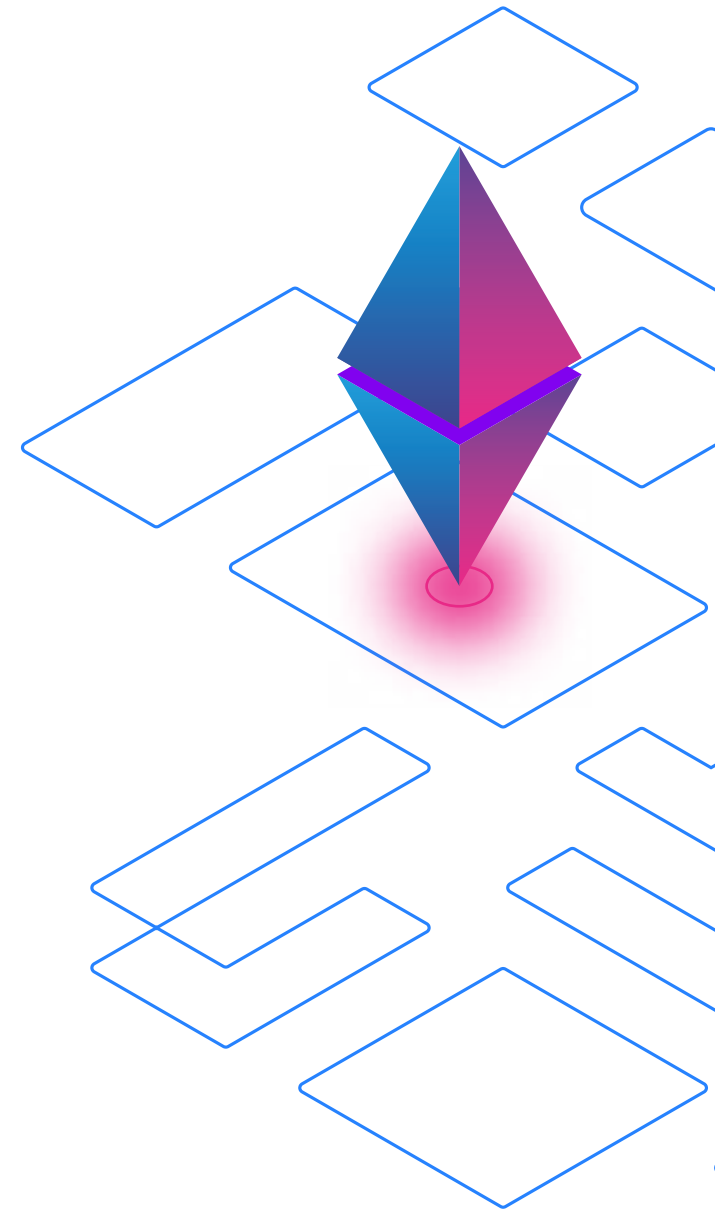
risks associated with the open source components used in your application. Software supply chain threats will continue to evolve, so businesses must constantly evaluate and re-evaluate their supply chain cybersecurity posture.

While our research proves that businesses are already embracing government regulations and directives, such as the Biden administration's Executive Order on Improving the Nation's Cybersecurity, there is a need to go further to improve software security and ultimately overall cybersecurity posture.

Companies must move beyond the implementation of SBOMs and use tools such as SCA to effectively manage and secure open-source and third-party software components to ensure comprehensive protection and resilience against software supply chain threats.

About the study

The research was conducted by Censuswide in May 2023. Censuswide surveyed a total of 217 IT Directors in large companies who oversee cybersecurity in organizations with a revenue of over £50 million/\$50 million in the UK and US markets respectively. In total, there were 102 UK and 115 US respondents.



About Sonatype

Sonatype is the software supply chain management company. We enable organizations to innovate faster in a highly competitive market. Our industry-leading platform empowers engineers to develop software fearlessly and focus on building products that power businesses. Sonatype researchers have analyzed more than 120 million open source components – 40x more than its competitors – and the Sonatype platform has automatically blocked over 145,000 malicious components from entering developers' code.

Enabling high-quality, secure software helps organizations meet their business needs and those of their customers and partners. Recognized by independent analysts as a leader, more than 2,000 organizations, including 70% of the Fortune 100 and 15 million software developers, rely on Sonatype's tools and guidance to be ambitious, move fast and do it securely. For more information, please visit [Sonatype.com](https://www.sonatype.com), or connect with us on [Facebook](#), [Twitter](#), or [LinkedIn](#).

