Foreward by: Cassie Crossley

Guidance by: Dmitry Raidman

SBOM

Accelerating Vulnerability Lifecycle Management with SBOMs

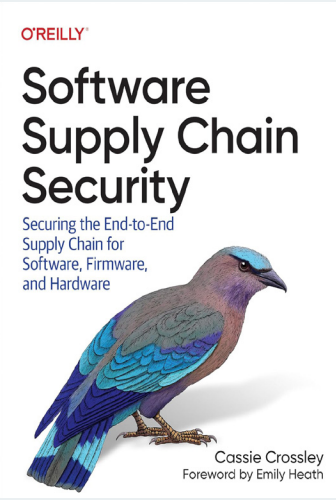
Contact us: info@cybeats.com

Foreword

Software is at the heart of nearly everything we do today. Whether we're talking about running a small business or managing a global enterprise, software is the engine that keeps the world moving. But with this reliance comes a vulnerability—a single flaw in the software supply chain can halt operations, compromise sensitive data, and cause significant financial damage. Securing that supply chain isn't just an IT problem; it's a business imperative.

In my work, I've emphasized that securing software is about more than just writing secure code. It's about understanding the entire supply chain—the people, processes, and technologies involved in bringing software from conception to deployment. This is where the concept of a Bill of Materials (BOM) becomes essential. Just as a manufacturer needs a BOM to track the components of a physical product, we need SBOMs, HBOMs, AIBOMs, and CBOMs to track and manage the components of our software, hardware, AI systems, and cryptographic protocols. These tools are not just about compliance; they're about visibility and control in an environment where the risks are increasingly complex.

What you'll find here is a detailed exploration of how to implement and manage these BOMs across the software lifecycle. This isn't just a technical guide—it's a strategic approach to mitigating risk, maintaining compliance, and ensuring that your software supply chain is resilient against the threats that we know are out there, and those that we have yet to encounter.



I've spent much of my career advocating for stronger supply chain security, and I'm encouraged to see how far we've come. But we're not done yet. The strategies outlined here represent the next steps in securing not just the code we write, but the entire process that delivers that code to the world.

I encourage you to think about how these practices can be integrated into your own processes. Whether you're in IT, development, procurement, or operations, your role is crucial. Together, we can build a more secure future, one where our reliance on technology is matched by our commitment to securing it.

–Cassie Crossley, Author of Software Supply Chain Security: Securing the End-To-End Supply Chain for Software, Firmware, and Hardware

Table Of Contents

Executive Summary

Securing the software supply chain is more important than ever as organizations increasingly rely on complex systems and third-party components. To address the full scope of security risks, it's essential to extend vulnerability management across the entire software lifecycle, from development through deployment. This approach, known as "shifting left and right," ensures that vulnerabilities are managed continuously and effectively.

Bills of Material (BOMs) play a key role in this strategy. Software Bills of Material (SBOMs) provide crucial visibility into software components, helping to identify and mitigate risks. Hardware BOMs (HBOMs), AI BOMs (AIBOMs), and Cryptography BOMs (CBOMs) serve similar purposes, offering detailed inventories of hardware components, AI systems, and cryptographic elements, respectively. These BOMs are essential for maintaining a strong security posture and ensuring compliance with an ever-expanding array of regulatory requirements.

Meeting these challenges requires practical solutions. Automating BOM management, integrating with existing security workflows, and continuously monitoring for vulnerabilities are all critical steps. Tools like Cybeats SBOM Studio provide the capabilities needed to implement these strategies effectively, ensuring that organizations can protect their software supply chains and meet the demands of modern regulatory environments.

Understanding and applying these practices enhances overall security posture and positions organizations to meet future challenges with confidence. Having SBOMs and automating SBOM management saves time, better utilizes scarce cybersecurity employees, and most importantly saves money.

76%
Improvement

500hrs
Saved Per Project

ICS

Cybeats has drastically reduced my vulnerability review and risk preparation time. For non open-source projects, I now save about 10 hours per project, and for open-source projects, the savings are around **500 hours per project**. The initial vulnerability list analysis time dropped from **15 minutes to 3 minutes** per vulnerability, and risk review preparation time went from **20 minutes to 5 minutes**. Cybeats has made our process more efficient and thorough.

Lead Cyber Security Engineer
(June 2024)

Introduction

Today's software is complex and vulnerable to cyber attacks. As companies build software using many parts from different sources, it becomes harder to spot and fix security problems. This is why we need better ways to manage vulnerabilities throughout the entire life of software.

Recent incidents underscore this need. For example, the SUNBURST attack, discovered by FireEye in December 2020, involved a sophisticated supply chain breach where attackers inserted malicious code into SolarWinds' Orion software. This affected thousands of customers and highlighted the critical importance of monitoring all components in software products. in early 2024, a backdoor was discovered in XZ Utils, a widely used data compression tool in Linux systems. This incident, known as CVE-2024-3094, involved a threat actor who spent two years gaining trust and becoming a maintainer of the project before implementing a backdoor in versions 5.6.0 and 5.6.1. The backdoor was designed to interfere with SSH authentication and allow remote code execution.

These attacks show how important it is to continuously monitor, quickly patch, and effectively respond to vulnerabilities in all parts of the software supply chain, including seemingly minor components that can have major security implications.

Most companies focus on finding and fixing security issues early in development. We call this "shifting left." But this approach isn't enough anymore. Once companies release software to customers, they often lose sight of new security problems. This creates a blind spot that attackers can exploit.

Cybeats recognizes that security doesn't end when a product is released. They tackle the problem of software vulnerability lifecycle management with the addition of a "shift right" approach. Shifting right means continuous monitoring and proactive management of security vulnerabilities, even after a software product is in production and in use by customers. This way, customers can quickly identify and mitigate risks, even as new vulnerabilities emerge over time.

Cybeats helps customers 'shift right'. Shifting right reduces risk as well as reduces costs by minimizing unscheduled/ unplanned work. –Duncan Sparrell of Fractal Consulting

Here's why this matters:

- It helps software makers track vulnerabilities in products their customers are using.
- It allows customers to stay alert about new vulnerabilities in software they've bought.
- It meets rules set by regulators, like the FDA's requirements for monitoring medical device security after sale.

How companies "shift right" depends on their relationship with customers. Some cloud services can update software directly. But often, customers decide when to update. In these cases, software makers must warn customers about serious vulnerabilities quickly.

Software Bills of Materials (SBOMs) are a key tool in this new approach. They list all the parts in a software product. This helps both makers and users of software find and respond to vulnerabilities faster. For users who control when they update, SBOMs help them stay vigilant about the security of software they're using.

Modern vulnerability management requires a comprehensive approach that spans the entire software lifecycle. By combining "shift left" and "shift right" strategies, organizations can better protect their software from development through deployment and beyond. The following sections will explore tools and methods for enhancing security across software, hardware, cryptography, and AI supply chains, with a focus on how different types of Bills of Materials improve transparency and security.

Understanding Bills of Material in Software and Hardware

Software Bill of Materials (**SBOM**)

A Software Bill of Materials (**SBOM**) is a tool that provides a detailed, machine-readable list of all the software components and dependencies in an application (NTIA, 2021). Think of an SBOM like an ingredient list on a food product—it shows exactly what's inside the software, which is important for managing and understanding the complexities of modern software supply chains.

In her book, "Software Supply Chain Security: Securing the End-To-End Supply Chain for Software, Firmware, and Hardware," Cassie Crossley, an expert in software supply chain security, emphasizes the scope of SBOMs:

> To understand SBOMs, you must first recognize that a product or service can be a combination of many components...there could be a thousand or more components and subcomponents within a single SBOM. –Cassie Crossley

Two main format standards have emerged for SBOMs: SPDX (Software Package Data Exchange) and CycloneDX.

Both are widely accepted in the industry:

- **CycloneDX** is designed for application security contexts and supply chain component analysis, supporting a wide range of use cases.
- **SPDX** is an open standard for communicating software bills of material information, including components, licenses, copyrights, and security references.

An SBOM includes several key elements. The **supplier name** tells you who made each component, making it easier to trace the source for updates, patches, or security alerts (NTIA, 2021). The **component name** and **version string** identify the specific parts used in the software, which is crucial when new vulnerabilities are found. If a vulnerability is reported, knowing the exact version helps you determine whether it's affected and needs immediate action.

Another important element is the **component hash**, a unique code that confirms each component hasn't been altered since it was included in the software. This ensures the integrity of the software and prevents tampering. Additionally, each component has **unique identifiers** that help track and manage software parts across different systems.

Finally, the SBOM maps out the **relationships** between components. This shows how different parts of the software depend on each other. If one component has a vulnerability, understanding these relationships helps you assess the potential impact on other parts of the software and decide how to respond (Cybeats, n.d.-a).

SBOMs help organizations manage vulnerabilities much more effectively. When a new security flaw pops up, teams can quickly check their SBOM to see if they're using the affected software. This speed saves precious time during potential security incidents. SBOMs also give security teams better information to make decisions about risks. They can see exactly what's in their software and understand how a vulnerability might impact their systems. This clear picture helps them decide what to fix first and how to protect their systems best. Overall, SBOMs cut down on the time and work needed to find and fix vulnerabilities. Instead of digging through systems manually, teams can use the SBOM as a map to guide their efforts, making the whole process faster and more efficient.

Hardware Bill of Materials (**HBOM**)

A Hardware Bill of Materials (**HBOM**) provides a detailed list of all the physical components used in creating and deploying a hardware device, such as integrated circuits, sensors, processors, and other electronic parts. HBOMs are essential for managing security risks in hardware supply chains. As hardware becomes more complex and interconnected, the risk of security vulnerabilities increases. Each component in a device can be an entry point for threats, making it crucial to maintain thorough documentation of every hardware element. This detailed tracking helps organizations identify and address potential risks, ensuring the security and integrity of their hardware systems (Cybeats, n.d.-c).

AI Bill of Materials (**AIBOM**)

An AI Bill of Materials (**AIBOM**) is an inventory that catalogs all components used in the development and deployment of artificial intelligence systems. This includes datasets, algorithms, models, frameworks, and third-party AI tools or libraries. The AIBOM is vital because it provides a clear and detailed map of AI system components, which is essential for identifying and mitigating vulnerabilities unique to AI. These vulnerabilities could include biases in training data or weaknesses in model architectures. By documenting every element of an AI system, organizations can better understand and manage the risks associated with their AI technologies, ensuring they operate securely and effectively (Department of Homeland Security, 2024).

Cryptography Bill of Materials (**CBOM**)

A Cryptography Bill of Materials (**CBOM**) is a detailed inventory of all cryptographic algorithms, protocols, and keys used within a software system. As the threat of quantum computing grows, current cryptographic standards may become vulnerable, making CBOMs increasingly important.

This concern is echoed at the highest levels of government. In August 2024, National Cyber Director Harry Coker Jr. addressed the critical nature of post-quantum cryptography at a White House event, stating: *"The migration to post-quantum cryptography is a complex undertaking that will take time, thought, and substantial work to implement"* (White House, 2024).

A CBOM allows organizations to identify cryptographic implementations that may be at risk in the face of quantum computing. It also helps plan for cryptographic agility, enabling smooth transitions to quantum-safe algorithms. Additionally, a CBOM ensures compliance with changing cryptographic standards and regulations, making it easier to manage the lifecycle of cryptographic assets. This proactive management is crucial for maintaining the security and integrity of cryptographic systems as technological threats evolve.

Interrelationships Between Different BOMs

Different types of BOMs—such as SBOMs, HBOMs, AIBOMs, and CBOMs—focus on specific aspects of a system, but they are often interconnected and complementary. For example, an SBOM might reference cryptographic libraries listed in a CBOM, or an AIBOM could include software components that are also documented in an SBOM. Understanding how these BOMs interrelate is key for managing vulnerabilities across complex systems. By integrating information from various BOMs, organizations can gain a holistic view of their security landscape, enabling more effective risk management and ensuring that all potential vulnerabilities are addressed comprehensively (Cybeats, n.d.-a).

The following comparison chart shows the distinct and complementary roles that the types of BOMs play in maintaining a secure and resilient technology environment.

Bills of Material Comparison Chart

Aspect	SBOM	AIBOM	CBOM	HBOM
Definition	Inventory of software components	Detailed inventory of AI components	Inventory of cryptographic algorithms, protocols, and keys	Inventory of hardware components
Primary Components	Libraries, frameworks, dependencies	Datasets, algorithms, models	Cryptographic algorithms, protocols, keys	Communication modules, Integrated circuits, sensors, processors
Key Benefits	Visibility, compliance, risk management	Transparency, bias detection, model integrity	Quantum-safe cryptography, regulatory compliance, cryptographic agility	Supply chain security, version control
Use Cases	Software development, vulnerability tracking	AI risk management, regulatory compliance	Cryptography management, quantum-safe planning	IoT security, hardware lifecycle management
Compliance & Regulatory Importance	NIST, ISO, EU CRA, DORA, PCI-DSS, FDA	NIST AI Risk Management Framework, EU AI Act	DHS Guidelines, NIST Post-Quantum Cryptography	NIST Cybersecurity for IoT, ISO/IEC 20243
Challenges	Integration with legacy systems, data accuracy	Rapidly evolving AI technologies, data privacy	Managing cryptographic transitions, ensuring key integrity	Tracking component provenance, ensuring integrity

Modernizing Vulnerability Management

Traditional Approach–Shift Left

In the past, vulnerability management primarily focused on identifying and addressing security issues early in the software development lifecycle, a strategy known as "shifting left." This approach centers on practices like secure coding, conducting static and dynamic code analysis, scanning for vulnerabilities early in the process, and gathering security requirements before development begins. By tackling security concerns at the outset, developers aimed to prevent issues from becoming more significant problems later in the lifecycle.

However, while shifting left is still crucial, it is no longer enough to manage the increasingly complex and evolving cybersecurity threats we face today. The focus needs to expand beyond the development phase to include the operational life of software products—a strategy known as "shifting right."

The Need for Shifting Right

Recent developments in cybersecurity have underscored the importance of extending vulnerability management beyond just the development phase. Shifting right involves continuing to monitor and manage vulnerabilities throughout the entire operational life of software. This shift is essential for several reasons:

Emerging vulnerabilities: New vulnerabilities can surface in components that were previously considered secure. For example, the Log4j vulnerability (CVE-2021-44228) affected numerous systems long after they had been deployed, demonstrating that security risks can emerge at any time.

Changing threat landscape: Cyber threats are constantly becoming more sophisticated and widespread. As noted by the Department of Homeland Security, the frequency and severity of cybersecurity threats, particularly in critical sectors like healthcare, have significantly increased, leading to greater potential for serious impacts.

Real-world exposure: Once software is deployed, it may encounter unexpected scenarios or configurations that were not anticipated during development. These real-world conditions can reveal new vulnerabilities that need to be addressed promptly to maintain security.

Regulatory compliance: Various regulations, such as the FDA's postmarket requirements, mandate continuous monitoring of vulnerabilities in deployed products. These regulations ensure that software remains secure throughout its entire lifecycle, not just during its development.

For software producers, shifting right ensures ongoing awareness of potential vulnerabilities in products being used by customers. For users, it provides the ability to be aware and respond quickly to newly discovered vulnerabilities in the software they depend on. By combining the strategies of shifting left and shifting right, organizations can create a more thorough approach to vulnerability management, addressing security threats both during development and throughout the software's operational life.

Achieving cybersecurity and resilience requires a secure supply chain and radical transparency, as the PCAST Cyber Physical Resilience Report and the National Security Memorandum on Critical Infr structure Security and Resilience highlight. Central to this transparency is the effective management of Bills of Materials (BOMs), which provides crucial insights into every component and dependency within the system (hardware, software, AI, crypto) ecosystem. –Dr. Georgianna Shea (Executive Office of the President, 2024)

Optimize Vulnerability Management Across the Lifecycle

BOM Management (SBOM, HBOM, AIBOM, CBOM)

Effective management of various Bills of Material (BOMs)—including Software (SBOM), Hardware (HBOM), AI (AIBOM), and Cryptography (CBOM)—is essential for vulnerability lifecycle management. Organizations must create accurate BOMs for all components in their systems and ensure these inventories remain updated throughout the product lifecycle. Maintaining up-to-date BOMs allows for better tracking of components, making it easier to identify and address vulnerabilities as they arise (Cybeats, n.d.-b). Secure distribution and version control are also critical. By securely sharing BOMs with relevant stakeholders and managing versions properly, organizations can prevent inconsistencies that might otherwise lead to security risks (NTIA, 2021).

SBOMs and VEXes are essential to protect the investment and the reputation of your brand, to reduce costs over the life of your products, and to instill confidence in your SDLC for customers and partners. –Dmitry Raidman

Vulnerability Discovery and Assessment

Continuous monitoring and scanning is required for the timely detection and assessment of vulnerabilities. This process includes real-time scanning to identify vulnerabilities as they emerge and integrating threat intelligence feeds to stay ahead of potential threats. Automated alerting systems play a vital role by notifying relevant stakeholders about critical vulnerabilities, allowing for swift action. Additionally, organizations must continuously track the software supply chain for new vulnerabilities in components. This proactive approach ensures that any risks are identified and managed before they can be exploited. Phil Englert (2024) emphasizes that continuous monitoring based on SBOM, which acts as a digital twin of the product's software, represents a new generation of tools that embrace the shift-left strategy.

Vulnerability Prioritization

Given the sheer volume of potential vulnerabilities, organizations must prioritize which to address first. This prioritization process involves several key factors:

- **CVSS score (v3.1/4.0):** The Common Vulnerability Scoring System provides a standardized severity rating for vulnerabilities.
- **CISA KEV catalog:** This catalog lists vulnerabilities that are actively being exploited in the wild.
- **EPSS:** The Exploit Prediction Scoring System predicts the likelihood of a vulnerability being exploited.
- **Existence of exploit proof-of-concept:** Indicates whether methods for exploiting the vulnerability are publicly available.

Weaponization status: Refers to whether the vulnerability has been incorporated into attack tools or frameworks like Metasploit.

Threat intelligence: Information on how specific threat actors are using vulnerabilities or targeting certain systems and market segments.

CISA SSVC: A system for prioritizing vulnerabilities based on their potential impact and exploitability. It takes into account factors like the vulnerability's technical impact, affected system's importance, and potential public harm if exploited.

Vulnerability Exploitability eXchange (VEX)

The Vulnerability Exploitability eXchange (VEX) is an emerging standard that complements SBOMs by providing additional context about the exploitability of known vulnerabilities in software components. VEX documents allow software suppliers or other parties to assert the status of specific vulnerabilities in a particular product (CISA, 2022). This information helps users prioritize their response to vulnerabilities based on their actual impact and exploitability.

Key elements of a VEX document include:

- Product identification
- Vulnerability identification
- Vulnerability status (e.g., affected, not affected, fixed, under investigation)
- Impact statement or action statement

VEX documents can be closely integrated with SBOMs and other types of BOMs to provide a more comprehensive view of a product's security posture. Combining BOM data with VEX information allows organizations to make more informed decisions about vulnerability management and prioritization (CISA, 2022).

Remediation and Mitigation

After identifying and prioritizing vulnerabilities, organizations need to take prompt action to address them. This often involves patch management, where security updates and patches are applied to vulnerable components. In cases where patches are not immediately available or applicable, organizations may implement compensating controls—additional security measures that reduce risk until a permanent fix can be deployed. These steps allow organizations to mitigate vulnerabilities and protect their systems from exploitation.

Reporting and Compliance

Organizations must also ensure robust reporting to meet both internal and regulatory requirements. They should use BOM data to demonstrate compliance with various standards and regulations. Effective reporting maintains transparency and accountability, ensuring that the organization adheres to necessary security protocols and industry standards (Cybeats, n.d.-b).

Overview of Key Regulations and Standards

The Regulatory Landscape

FDA 510(k) Pre-Market and Post-Market Requirements: The FDA mandates comprehensive documentation and ongoing monitoring for medical devices, which SBOMs support by providing detailed visibility into software components, helping to ensure their safety and effectiveness.

EU CRA (Cybersecurity Act): The European Union's Cybersecurity Act highlights the need for transparency in software supply chains, advocating practices that align with the creation and maintenance of SBOMs.

NIST SSDF (National Institute of Standards and Technology Secure Software Development Framework): The NIST SSDF emphasizes the importance of SBOMs for managing software security risks and ensuring compliance with federal requirements.

PCI-SSF (Payment Card Industry Software Security Framework): The PCI-SSF provides a set of security standards for software development and maintenance, emphasizing the importance of secure coding practices, regular security assessments, and the use of SBOMs to ensure that all software components are documented and managed properly.

PCI-DSS (Payment Card Industry Data Security Standard): PCI-DSS includes requirements for securing software applications, which can be effectively met through the use of SBOMs.

DORA (Digital Operational Resilience Act): This act mandates financial entities in the EU to ensure their digital systems are resilient, which includes maintaining detailed records of software components.

NIS2 (Network and Information Systems Directive): The NIS Directive requires operators of essential services and digital service providers to take appropriate security measures, including maintaining SBOMs.

ISO (International Organization for Standardization): ISO standards for software security include provisions for documenting and managing software components, aligning closely with the principles of SBOMs.

ISA/IEC 62443-4-1 (North American Electric Reliability Corporation): This international standard focuses on secure product development lifecycle requirements for industrial automation and control systems. It emphasizes the importance of managing third-party components and libraries throughout the software development process.

NERC Guidelines (International Society of Automation/International Electrotechnical Commission): Guidelines for cybersecurity in the electricity sector. These guidelines increasingly emphasize the importance of software supply chain security, including the use of SBOMs to manage and monitor software components in critical infrastructure systems. NERC's approach aligns with industry best practices for maintaining the reliability and security of the power grid.

DHS (Department of Homeland Security): The DHS recommends using SBOMs and AIBOMs to manage risks in AI and software supply chains, ensuring the security of critical infrastructure through robust testing, continuous monitoring, and transparency (Department of Homeland Security, 2024).

The Securities and Exchange Board of India (SEBI) issued a Request for Proposal (RFP) in July 2024 for the "Implementation and Operation of Vulnerability Management (VM) Solution at SEBI," requiring bidders to provide a "Detailed Technical Bill of Material (BOM)." This move highlights SEBI's focus on software supply chain security, aligning with SBOM principles.

The Ministry of Economy, Trade and Industry (METI) of Japan published the "Guidance on the Introduction of the Software Bill of Materials (SBOM) for Software Management" in July 2023. This document provides guidance on implementing SBOM, indicating growing government interest in the concept and covering various aspects of SBOM, including its benefits, myths, and practical steps for implementation.

The National Intelligence Service (NIS), the Ministry of Science and ICT (MSIT), and the Presidential Committee on the Digital Platform Government (DPG) of South Korea jointly released the "Software Supply Chain Security Guidelines 1.0" in May 2023. This document introduces the SBOM method for the first time in the country, providing guidance for developers, suppliers, and management companies on creating and managing SBOMs to track software vulnerabilities.

Failing to comply with EU CRA Software Bill of Materials ("SBOM") reporting could lead to a €15 million (approximately $16.3 million USD) administrative fine, or 2.5% of an organization's gross sales, whichever is higher. – Chuck Brooks

Role of BOMs in Regulatory Compliance

Different types of BOMs play key roles in meeting various regulatory requirements:

- **SBOMs** support compliance efforts by providing transparency into software components and facilitating vulnerability management (Cybeats, n.d.-b).
- **HBOMs** are important for hardware-related regulations, helping organizations track and manage physical components in their systems.
- **AIBOMs** are essential for compliance with AI-specific guidelines, such as those issued by DHS (Department of Homeland Security, 2024).
- **CBOMs** facilitate cryptographic compliance requirements, especially as organizations prepare for the post-quantum era (IBM Research, n.d.).

VEX and Regulatory Reporting Requirements

The Vulnerability Exploitability eXchange (VEX) is a standardized framework that helps software vendors and security teams communicate the status and impact of vulnerabilities in their products. VEX documents are machine-readable and provide clear information about whether specific vulnerabilities affect particular products and what the potential impact might be.

Several formats support VEX, with two of the most prominent being CSAF 2.0 Profile 5 and CycloneDX. CSAF (Common Security Advisory Framework) 2.0 Profile 5 is designed specifically for VEX use cases, while CycloneDX is a popular format for Software Bill of Materials (SBOM) that also supports VEX data. These formats, along with others in the industry, help standardize how organizations share vulnerability information.

VEX is designed for software vendors, security teams, and regulatory bodies. Vendors use VEX to inform customers whether their products are vulnerable, helping them prioritize security efforts. Security teams rely on VEX to focus on vulnerabilities that are confirmed to be exploitable, avoiding unnecessary mitigation efforts. Regulatory bodies use VEX to ensure organizations meet their obligations to manage and report vulnerabilities accurately.

VEX is important because it provides context to raw vulnerability data, allowing organizations to focus on actual threats. It helps avoid unnecessary work on vulnerabilities that don't pose a risk. Additionally, VEX supports regulatory compliance by offering a consistent way to report on vulnerability status and impact, which is increasingly required by global cybersecurity regulations (CISA, 2022).

Challenges in Multi-jurisdiction Compliance

Organizations often face challenges in complying with regulations across multiple jurisdictions. A comprehensive approach to BOMs and vulnerability management can help address these challenges by providing a unified view of system components and their security status.

Future Trends in Regulatory Requirements

As cyber threats continue to advance, regulatory requirements are likely to become more stringent and comprehensive. Organizations that implement robust vulnerability lifecycle management practices now will be better positioned to meet future regulatory challenges.

Best Practices for Effective Vulnerability Management

Implementing effective vulnerability management requires a comprehensive approach that integrates people, processes, and technology. Organizations must establish a clear vulnerability management policy that defines roles, responsibilities, and procedures for identifying, assessing, and remediating vulnerabilities. This policy should serve as the foundation for all vulnerability management efforts. Continuous monitoring is crucial, so organizations should deploy automated tools that continuously scan all systems and components for vulnerabilities (Phil Englert, 2024).

To prioritize vulnerabilities effectively, organizations should adopt a risk-based approach that takes into account factors such as CVSS scores, exploit availability, and business impact. Regularly updating SBOMs, HBOMs, AIBOMs, and CBOMs ensures accurate visibility into system components, which is essential for managing risks (Cybeats, n.d.-a).

Fostering a security-aware culture is also key; organizations should provide regular training and awareness programs for all staff involved in software development and operations. Additionally, collaborating with vendors and the broader security community enhances the organization's ability to respond to emerging threats by participating in information-sharing initiatives and maintaining open communication channels with software and hardware vendors.

Choose the Right Tools for Success

Selecting the right vulnerability management tools can make or break your security efforts. The right solution will streamline your processes, improve your threat detection, and help you respond faster to emerging risks. Without effective tools, you'll struggle to keep up with the constant stream of new vulnerabilities and potential threats. Here are the key factors to consider when choosing your vulnerability management platform:

Integration capabilities: Choose tools that seamlessly work with your existing systems

Automation features: Look for platforms that automate repetitive tasks

BOM management: Ensure the solution can handle various types of BOMs and keep them current (Cybeats, n.d.-c)

Scalability: Select tools that can grow with your organization's needs

Reporting and analytics: Opt for solutions with comprehensive insights to support decision-making

Integrate Vulnerability Management into DevSecOps

To achieve effective "shift-right" capabilities, organizations must integrate vulnerability management into the entire DevSecOps lifecycle. During the development phase, security testing and vulnerability scanning should be incorporated into the process to catch issues early. In the Continuous Integration/Continuous Deployment (CI/CD) phase, organizations should automate vulnerability scans as part of the pipeline to ensure that new code doesn't introduce new risks. Once software is in production, continuous monitoring and automated patching are essential for maintaining security. Establishing a feedback loop that feeds vulnerability information back into the development process is needed for continuous improvement.

Discover Cybeats SBOM Studio

Cybeats SBOM Studio helps organizations manage and analyze software security risks throughout a product's lifecycle. By working well with tools companies already use, Cybeats helps teams spot and fix security issues quickly and meet industry rules. This gives companies more control over their software supply chain.

Cybeats doesn't create SBOMs, but instead partners with various SBOM creation tools through its BCA Marketplace. This approach offers a flexible and thorough way to secure your software supply chain, letting you use your preferred SBOM tools while benefiting from Cybeats' powerful management and analysis features.

Key features and capabilities:

1. **SBOM management and integration:** Through its BCA Marketplace, Cybeats connects with various SBOM creation tools. This means you can use your favorite SBOM generation tools and then use Cybeats to manage and analyze those SBOMs. By connecting with many SBOM sources, Cybeats helps you keep a complete, up-to-date list of all your software parts, including where they came from and what they depend on. This saves time and reduces mistakes.

2. **Finding and ranking vulnerabilities:** The platform constantly looks for new security weaknesses in all the software parts listed in your SBOMs. It uses threat information and risk assessment tools to decide which vulnerabilities are most important. This helps you fix the biggest security problems first, lowering your risk of attacks and using your resources wisely.

3. **Meeting industry compliance:** As regulations get stricter, following the rules becomes more important. Cybeats SBOM Studio shows you clearly what's in your software and how secure it is. This makes it easier to meet standards like FDA, ISO, and EU Cybersecurity Act.

4. **Working with development and security tools:** Cybeats SBOM Studio fits in smoothly with the tools developers and security teams already use. This helps catch and fix security issues at every stage of software development, from when code is first written to when it's being used by customers.

5. **Reports and analysis:** To help you make smart decisions, Cybeats SBOM Studio gives you strong reporting and analysis tools. It shows you how secure your software parts are, trends in vulnerabilities, and how well you're fixing problems. This information helps you improve your security strategies over time.

Of note, Cybeats is launching a new product called SBOM Consumer, currently in beta. This tool is designed for organizations that use software from various suppliers rather than developing it themselves. SBOM Consumer allows you to import SBOMs from your software suppliers and view them all through an easy-to-use interface. It shows all vulnerabilities and continuously monitors your specific environment for new issues. The tool is affordable and will integrate in the future with your existing asset management systems. While traditional asset discovery tools look at devices from the outside, SBOM Consumer gives you in-depth visibility into the ingredients of software based products. This approach is particularly useful for consumers of software who don't need to generate SBOMs but want to leverage the SBOMs provided by their suppliers to enhance their security posture.

How Cybeats Addresses Vulnerability Management Challenges

Cybeats SBOM Studio tackles several key challenges in modern vulnerability management. Its continuous monitoring and management of SBOMs allow organizations to maintain visibility into their software supply chain throughout the entire product lifecycle (Cybeats, n.d.-b). This ongoing insight is necessary to address the dynamic nature of software security.

Cybeats now supports not only Software Bills of Material (SBOMs), but also AI Bills of Material (AIBOMs), Hardware Bills of Material (HBOMs), and adding support for Cryptography Bills of Material (CBOMs). This expanded capability provides organizations with a holistic view of their system components, offering a more comprehensive understanding of potential vulnerabilities and risks across various aspects of their technology stack.

The platform's multi-BOM support helps organizations meet regulatory requirements by providing detailed information about software, hardware, AI, and cryptographic components and their security status. This enables companies to demonstrate compliance more effectively across a wide range of regulatory frameworks. Cybeats also supports the integration of Vulnerability Exploitability eXchange (VEX) documents for more context-aware vulnerability management, allowing organizations to better understand and prioritize their security efforts.

Designed to handle large-scale environments, Cybeats SBOM Studio automates many aspects of vulnerability management. This automation can significantly reduce manual effort and improve overall efficiency in security operations. Cybeats gives teams the tools they need to spot and fix vulnerabilities quickly throughout their supply chain. By using Cybeats, organizations can take charge of their security instead of just reacting to problems after they happen.

By implementing rigorous BOM management, organizations gain the visibility needed to proactively identify and address vulnerabilities, thereby enabling swift and effective risk mitigation throughout the entire lifecycle of their systems.

This approach begins with securing the supply chain and extends through all stages of the system and software lifecycle, ensuring that vulnerabilities are managed comprehensively and security and resilience are maintained at every level. —Dr. Georgianna Shea (Executive Office of the President, 2024)

How to Choose the Right SBOM Solution

When you're looking at specific solutions like Cybeats SBOM Studio, see how they handle these factors and fit with your company's unique needs and current processes. Remember, you want to find a solution that not only works for you now but can also adapt as your needs change in the future.

Think about these key factors:

1. **Technology environment:** Look at your company's tech setup. Do you use embedded systems (computers built into other devices), cloud services, or different kinds of apps? Your SBOM tool needs to work well with what you already have. Think about the coding languages and frameworks your team uses. A good solution should handle all the tech you work with.
2. **Software components:** Check what makes up your software. Do you use a lot of open-source code (freely available software)? Do you buy pre-made commercial software? Or do you have custom code made just for you? Pick an SBOM solution that can track all these different types of software parts.
3. **Existing tools:** Your team probably uses other development and security tools already. Maybe you use Black Duck to manage open-source code, or you work with GitHub or GitLab for coding. Choose an SBOM solution that works well with these tools. This will make it easier for your team to start using it without changing how they work.
4. **SBOM generation methods:** You can create SBOMs in different ways. You might use free, open-source tools, buy a solution from a company, or even make SBOMs by hand. Some platforms, like Cybeats' BCA Marketplace, offer several options. Think about what works best for your team. Do you need the flexibility of open-source tools, or would a more polished commercial solution fit better? Consider how accurate each method is, how easy it is to use, and how well it fits into your current way of working.
5. **Scalability and integration:** Your SBOM solution should grow with your company. If you're small now but plan to get bigger, make sure your chosen solution can handle more complex and larger-scale operations over time. Look for tools with good APIs (ways for different software to connect) and integration features. These will help your SBOM solution work smoothly with your other tools and processes.
6. **Compliance and standards:** Following rules and standards is important. Make sure your SBOM solution supports common formats like SPDX and CycloneDX. It should also help you meet any rules specific to your industry. Whether you work in healthcare, finance, or another regulated field, your SBOM solution should make it easier to follow the rules.
7. **Ongoing management:** Creating SBOMs is just the start. You need a solution that helps you manage them over time. Look for features that keep your SBOMs up-to-date automatically. The software world changes fast, and your SBOM solution should keep up. It should also help you find and manage security weaknesses, turning your SBOMs into a powerful tool for ongoing risk management.

Forward Outlook

As the complexity of software systems continues to grow and cyber threats evolve, effective vulnerability lifecycle management will become increasingly important. The shift towards comprehensive approaches that encompass both “shifting left” and “shifting right” represents a significant step forward in addressing these challenges.

The use of various Bills of Material (SBOMs, HBOMs, AIBOMs, and CBOMs) along with emerging standards like VEX provides organizations with powerful tools to manage their software supply chains and address vulnerabilities more effectively. As regulatory requirements become more stringent, these tools will play a crucial role in ensuring compliance and maintaining robust cybersecurity postures.

Looking ahead, we can expect to see further integration of artificial intelligence and machine learning into vulnerability management processes, enabling more predictive and proactive approaches. The growing importance of quantum-safe cryptography will also likely drive increased adoption of CBOMs and related tools.

Organizations that invest in vulnerability lifecycle management solutions now will be better positioned to face the cybersecurity challenges of the future, ensuring the safety, security, and resilience of their critical systems and infrastructure. are Supply Chain Security: Securing the End-To-End Supply Chain for Software, Firmware, and Hardware.

LEARN MORE

5
New Metrics

10x
From Days to Hours

Cybeats has given us new capabilities and improved our visibility into third-party and open-source software. Leveraging on their SBOM Studio, we could track the software supply chain down to the root libraries in our containers. This allowed us to report on **5 new metrics to our management**. Cybeats were found to have a **higher true positive rate than competing OSA** and container analysis tools. Combined with the detailed vulnerability analysis presented in an easy-to-read manner, we shortened our vulnerability review timeframe **from a day to under an hour**. It is our go-to tool and we now know where to focus our limited security resources next.

Lead Security Architect, Product Supply Chain Security (June 2024)

Published by CyBeats Technologies Inc.