

SOFTWARE SUPPLY CHAINS: A MAJOR CHALLENGE FOR CYBERSECURITY

WHITE PAPER



SUMMARY

The protection of software supply chains from attackers is one of the most pressing cybersecurity issues that we face today. Massive security incidents arising from software vulnerabilities demonstrate that serious threats can spread via a supply chain to impact multiple parties.

Cyberattacks that target governments and organizations are on the rise. In recent years, attackers have infiltrated government infrastructure, compromised private companies and accessed colossal amounts of sensitive data. A hacking campaign in 2020 targeted a vulnerability in SolarWinds software and managed to penetrate US government departments including the Department of Homeland Security and part of the Pentagon.

For businesses, attacks on software supply chains can lead to the loss of key data and intellectual property, significant interruption to their operations, heavy financial losses and a devastating impact on reputation. These impacts can be passed on to customers along the chain.

In May 2021, US President Joe Biden responded to threats like the SolarWinds hack with the release of Executive Order 14028 on Improving the Nation's Cybersecurity.

It enforces measures to strengthen software supply chains, thereby reducing the risks involved for the federal government system and improving cybersecurity across the industry.

In recent years, similar legislation has been created in Australia (The Security Legislation Amendment [Critical Infrastructure Protection] Act 2022), the UK (the Network



and Information Systems (NIS) regulations of 2018), Europe (the proposed Cyber Resilience Act.), and in Canada (the proposed Bill C-26, An Act Respecting Cyber Security, which also extends to federally regulated industries).

This new legislation sets out to protect all parties who depend on a secure and monitored supply chain. When a supply chain is insecure, organizations take on substantial risk as consumers of products and software. As providers and producers themselves, organizations pass on this risk to consumers.

However, our research shows that despite the catastrophic impact of cyberattacks, most software supply chains remain underprotected.

As consumers, organizations trust open-source software producers, third-party software providers and the hosting providers with whom they build their infrastructure without knowing exactly how they function.

In many cases, an organization that provides software to consumers might have a software producer they weren't aware of in their own supply chain. There might be third-party software libraries concealed within the software that they consume or provide to other parties.

Despite the stakes in play, most organizations also lack a central communications solution to exchange updates with partners and consumers when a cybersecurity incident inevitably occurs. This is complicated by the need to coordinate with other vendors when disaster strikes.

Some vulnerabilities within software systems are known as "zero-day" because developers have exactly that amount of time to fix the problem before it's exploited by hackers. The irony emphasizes the fact that when the developer spots a vulnerability, the chances are that someone else has already found it—and has made their attack.

When software vendors are unaware of vulnerabilities, or don't communicate them to other members of their supply chain, the clock is already ticking, and a critical security situation develops.

It's only ever a matter of time before the next headline software vulnerability is exposed. So, it's imperative for IT decision makers to monitor their software supply chain regularly and plan how to respond quickly in order to reduce the damage to their organization in the event of a security breach.

ABOUT THE STUDY

BlackBerry asked 1,500 senior IT decision makers and cybersecurity leaders about how they managed the risk of security breaches from their supply chains.

The respondents came from North America, Australia and the UK, with job titles including Chief Technology Officer, Director of Threat Intelligence, Head of Infrastructure and Head of IT.

They were cybersecurity leaders for organizations across all sectors: professional services, retail, hospitality and travel, education, telecommunications, healthcare, energy, media and internet, banking and finance, transportation, and technology and software. Of those in technology and software, 66% supplied software to government departments.

They worked for mid-size organizations: the average annual revenue of their workplaces was \$674,000,000, with 12% turning over \$1,000,000,000 or more. The average number of employees at their organizations was 1,917.

KEY FINDINGS



80% of organizations had been notified of a vulnerability or attack within the supply chain of software they consume in the last 12 months.

The ubiquity of these alerts is concerning considering the stakes involved. Respondents whose supply chain was the target of an attack suffered significant operational disruption, data loss and impact to the reputation of their organization.

- 77% of organizations uncovered hidden members of their software supply chain that they had not previously been aware of in the last 12 months.

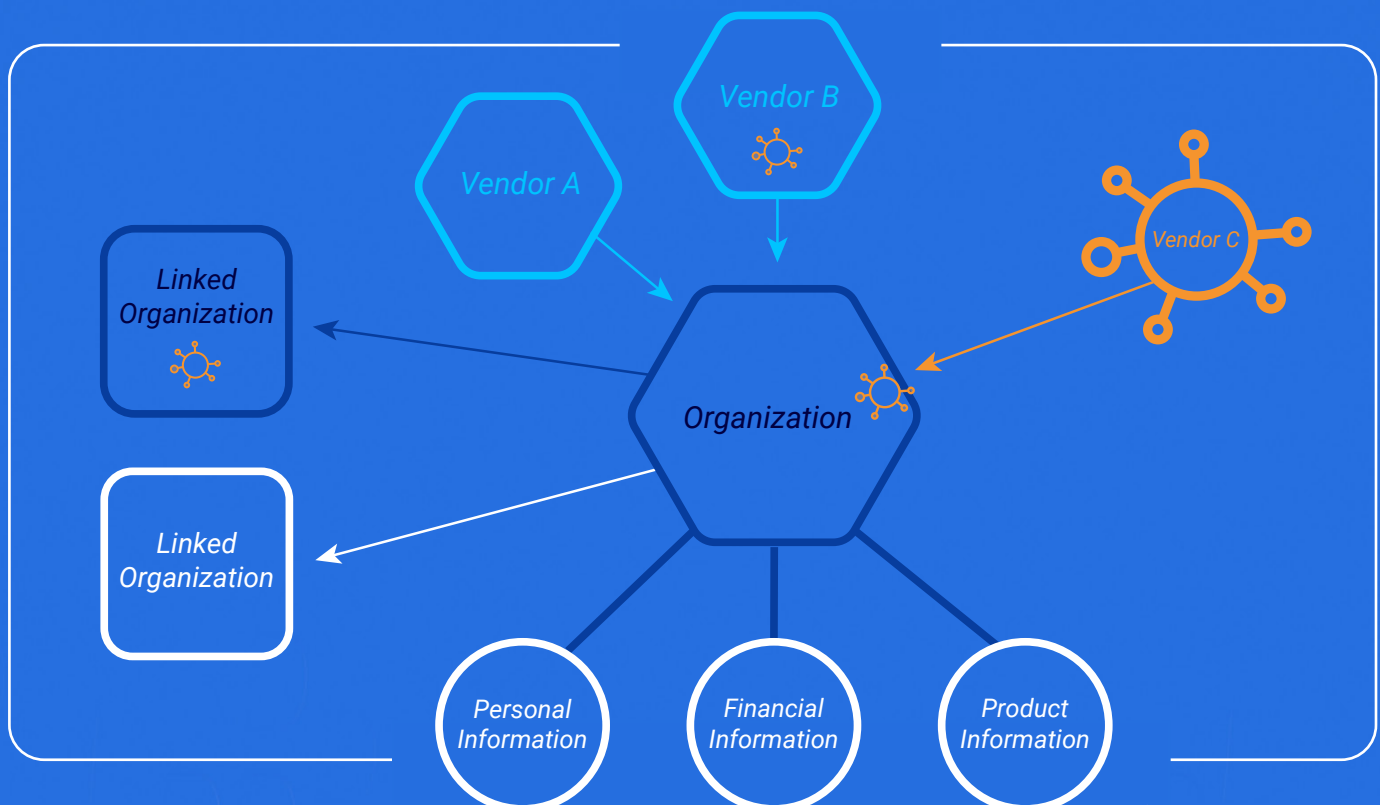
If businesses are not aware of every member of their software supply chain, from corporate entities to software libraries, they may fail to spot vulnerabilities which cyberattackers could exploit to compromise their systems.

- 62% of organizations say speed of communication is paramount during a cyberattack.

Organizations know they can mitigate some of the damage caused by a cyberattack by responding promptly. However, only 19% have a single effective channel in place that they can use to alert key stakeholders when their systems are compromised.

- 72% of respondents call for greater government oversight of open-source software to increase cyber protection.

WHAT IS A SUPPLY CHAIN ATTACK?



The decentralized model of open-source software is the foundation of much of today's digital world. Are organizations starting to question the value of this model? The ramifications of governmental oversight of open-source software might not be what you'd expect.

CASE STUDY: LOG4J

Towards the end of 2021, a critical security flaw was found in a popular software library called Log4j, distributed by the Apache Software Foundation. Part of the Java programming language, Log4j helps software applications log their past activities.

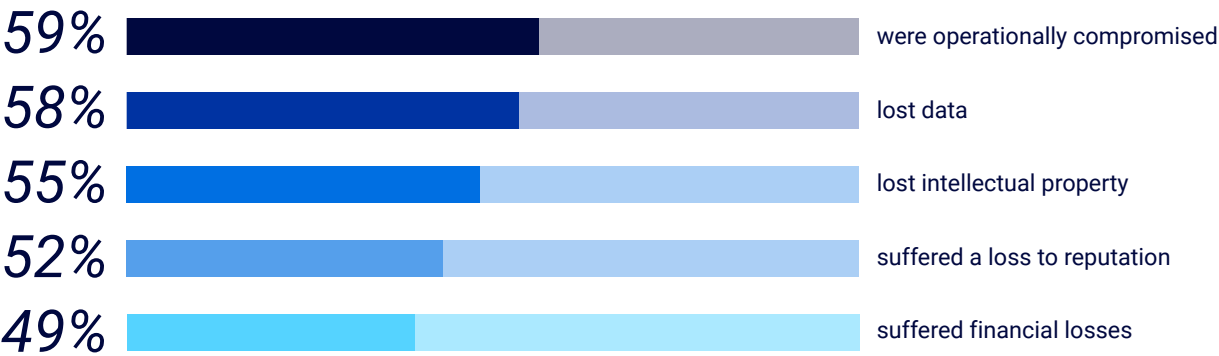
Java is one of the most popular programming languages and directly or indirectly, 95% of Java programs use Log4j. Commentators called the vulnerability “a severe risk to the entire internet”.¹ In the first 72 hours after the vulnerability was discovered, cybersecurity experts detected over 800,000 attempts to exploit it.

It was a crisis that spread across the technology industry. Attacks were detected across retail, technology, manufacturing, financial services and government organizations. Most software vendors were impacted, since even if the vulnerability wasn't in the software they produced, it was in their supply chain. The issue remains endemic as not all vulnerabilities have been patched—or discovered.

THE IMPACT OF CYBERATTACKS

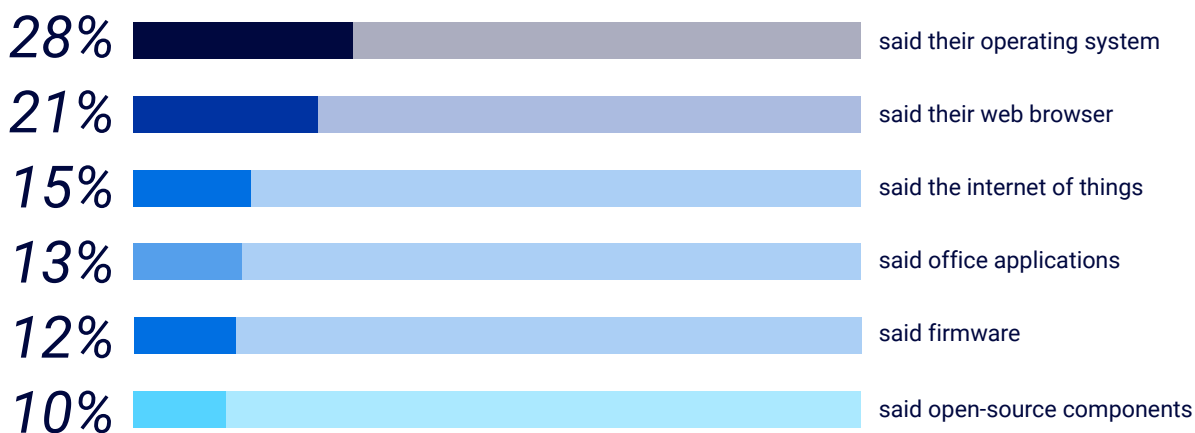
In the last year, four out of five of the organizations we surveyed had been notified of a vulnerability or attack within the supply chain of the software they consume.

The impact of these vulnerabilities can be severe. Following an attack, of the organizations we surveyed,



TARGETS WHERE THE BIGGEST IMPACT WAS FELT

Organizations were asked where, across their systems, vulnerabilities had the most impact.



In nine out of ten organizations, operations took up to a month to recover following a software supply chain attack. The damage to reputation and brand lasts much longer.

SECURITY INSIDE YOUR ORGANIZATION

66% of IT decision makers and cybersecurity leaders believe that cybersecurity policies across their supply chain are comparable to those in place at their company. But a closer look at these organizations reveals that internal cybersecurity is far from watertight, which means they have set a low bar for their supply chain.

When it came to vulnerabilities in the software they produce, 15% of respondents did not track the impact on their downstream consumers. The majority of organizations do monitor and report on these risks. However, when even a few do not, the security implications could be significant.

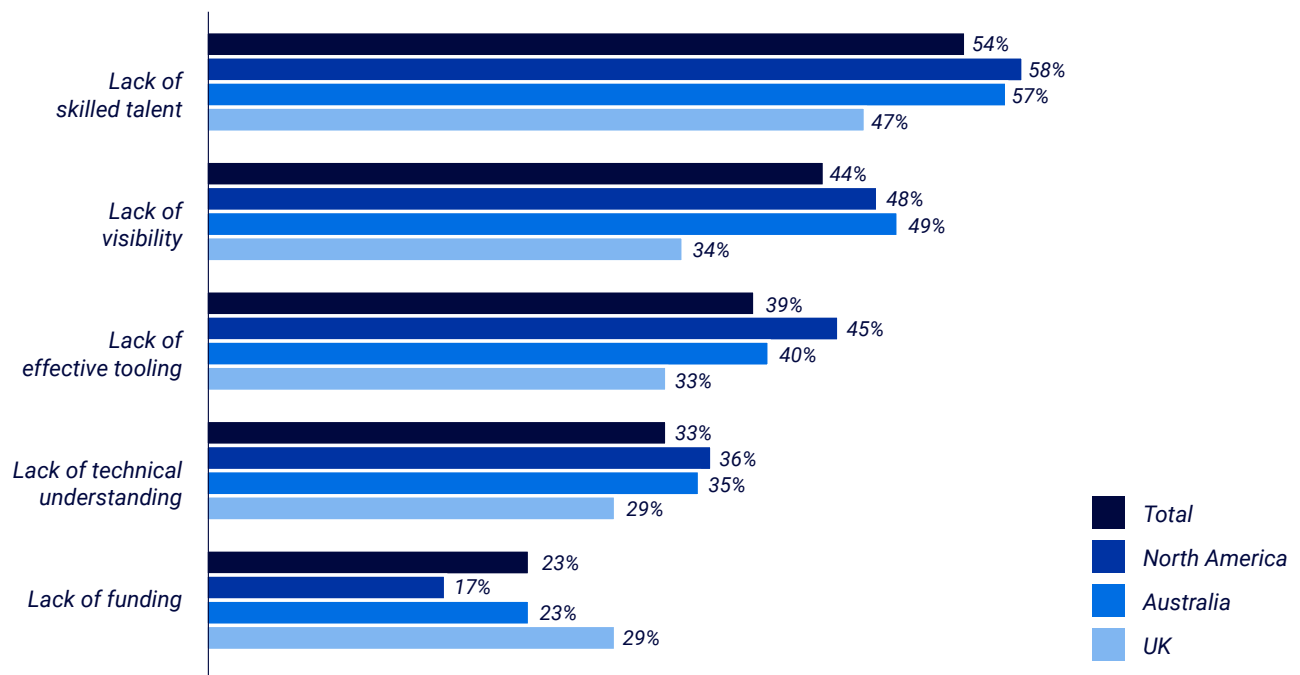
Timeliness is another key issue for organizations. When vulnerabilities are uncovered, it's important to respond quickly. Imagine if your organization's functions, knowledge

and reputation were safeguarded in a private office of your building. A software vulnerability that isn't patched leaves the door to that private office unlocked.

It might be considered surprising, then, that on average, senior IT decision makers and leaders perform an inventory of their own software environment only every three months. In comparison, they recognize that speed of response is key when a partner suffers a security breach. In the event of a breach in their supply chain, they would expect to be notified within 13 hours.

So, why don't organizations perform more regular software inventories? One key barrier is identified by over half of organizations: 54% named a lack of skilled talent. This response may underrepresent a skills gap across organizations: 33% named a lack of technical understanding as the main factor preventing them from performing regular checks of their software infrastructure.

WHAT ARE THE BIGGEST BARRIERS TO REGULAR SOFTWARE INVENTORIES?



Multi code question
Base: All respondents (1,500) North America (500), Australia (500) UK (500)
Coleman Parkes Research

Instead, the majority of organizations rely on security awareness and cybersecurity best practice employee training to safeguard their systems. Almost half ensured they were using endpoint detection and response to uncover stealth attackers, some having logs monitored by a security operations center. More than a third employed vulnerability tracking and reporting. Fewer organizations relied on their current software policies, set up an open-source program office or employed a patch management strategy.

MONITORING YOUR SUPPLY CHAIN

When organizations seek to conduct an inventory of their supply chain, and ensure they have a complete account of the partners, providers and software they rely on to function, the greatest number (20%) are doing so in order to identify potential threats. An additional 10% are doing so to access third-party threat intelligence, presumably in response to a security alert.

A chain is no stronger than its weakest link. The senior IT decision makers and cybersecurity leaders whom we surveyed were making an effort to perform due diligence when it came to their supply chains.

The most popular measures that organizations insisted their supply chains had in place were data encryption (63%) and identity access management controls (56%), with the least popular being zero-trust architecture (19%) and honeytokens (15%).

When using honeytokens, it may be a challenge to create a type of bait that an attacker can't resist, yet ensure that targeting it cannot benefit them. Perhaps this complexity is the reason that this is a much less popular defense method.

Other security methods that organizations insisted upon from their supply chains, from most to least popular, were a secure privileged access management framework, compliance with secure software development practice, vulnerability reporting, staff training on cyber awareness protocols, a third-party data platform or software, a Software Bill of Materials (requested during procurement) and vendor network monitoring.

Organizations are clearly doing their best to secure their supply chains, both as providers and consumers, using a variety of strategies in the hope of achieving the best possible defense against attackers. But nevertheless, IT experts could have grounds for concern about some aspects of their approach to cybersecurity.

GAPS IN OVERSIGHT

In the last 12 months, 77% of organizations uncovered hidden members of their software supply chain of which they had not previously been aware. They had not been monitoring these partners, providers and software components for critical security standards.

"It is the lack of granular detail that exposes vulnerabilities for cybercriminals to exploit," said Christine Gadbsy, VP, Product Security at BlackBerry.

These gaps in oversight reflect a lack of knowledge and confidence around how to identify and prevent security breaches in supply chains. Almost a quarter of organizations surveyed (22%) said they had only limited knowledge of how they would manage this risk. 29% of organizations were only somewhat confident, or not confident at all, that their suppliers and partners could identify vulnerabilities in their software environment and prevent them being exploited.

When asked what sector of their supply chain and partner network they were least confident was secure, 30% named open-source software producers, while 25% named financial or e-payment solution providers.

21% were concerned about third-party software providers, 15% about transport and logistics partners, and 10% about manufacturing partners.

Organizations who want to monitor the other parties in their supply chain can choose from a number of options: software component cataloging and tracking, or deploying software that deals with issue management or customer experience management.

Gadbsy emphasized that gaps in surveillance of the attack surface of the software that an organization produces and consumes could cause significant issues.



3 in 4
*businesses uncovered **hidden**
members of their **supply chain**
that they were previously
not aware of.*

“Unknown components and a lack of visibility on the software supply chain introduce blind spots containing potential vulnerabilities that can wreak havoc across not just one enterprise, but several, through loss of data and intellectual property, operational downtime along with financial and reputational impact. How companies monitor and manage cybersecurity in their software supply chain has to rely on more than just trust.”

Considering the severity of potential problems, speed is of the essence when an organization becomes aware of a vulnerability that might impact its software supply chain. Software producers should urgently contact consumers so that they can manage the impact. On average, when alerted about a cybersecurity breach, organizations took two days to identify if an impacted library was used in any of the software they consumed.

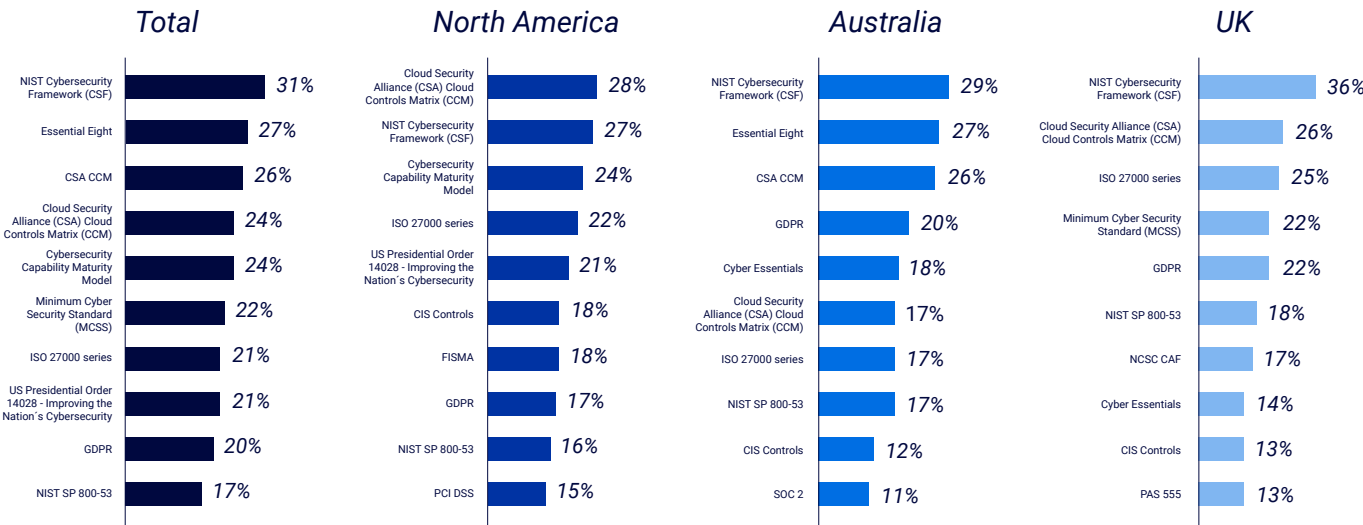
A PATCHWORK OF REGULATION AND COMPLIANCE

A third of senior IT decision makers and cybersecurity leaders within organizations are only somewhat confident (31%) or not confident (2%) that their supply chain partners have adequate cybersecurity regulatory and compliance practice.

But organizations make an effort to perform due diligence by checking which risk management and security control frameworks their partners and suppliers adhere to. For example, a partner who adheres to the NIST Cybersecurity Framework will have multi-factor authentication enabled to their build chain, meaning that an organization can be confident that their build infrastructure won't be compromised (as happened in the SolarWinds hack, which affected the data, networks and systems of thousands of organizations—and through them, their customers and partners).

On average, organizations audit their suppliers and partners against these frameworks every eight months. Rather than performing more frequent checks, organizations tend to rely on an assurance from a supply chain partner that these controls are in place.

WHAT RMFS/ SECURITY CONTROL FRAMEWORKS DOES YOUR ORGANIZATION ADHERE TO?



Multi code question
Base: All respondents (1,500) North America (500), Australia (500) UK (500)
Coleman Parkes Research

Top 10 answers shown

COMMUNICATIONS CHALLENGES

When a zero-day or other highly publicized vulnerability makes headlines, organizations rush to understand if they are impacted.

If a vulnerability affects a software supply chain, organizations agree that it's crucial to contact key stakeholders fast. 62% said that speed is the most important aspect of communicating with the partners, clients and customers in the chain. 53% said it was most important for roles and responsibilities to be clearly defined, 44% emphasized clarity of communication and 35% highlighted active engagement with stakeholders.

The expectation of speed goes both ways: organizations expected their supply chain partners to contact them within 13 hours with a security alert in the event of a cyber breach.

Despite prioritizing speed and clarity, 81% of organizations use multiple communication systems to raise the alarm when their supply chain is compromised. In the event of a zero-day attack, or attackers exploiting a known vulnerability, it seems that the use of a single communication system would have clear advantages.

Using a single secure back channel, organizations would be able to get the message out to all stakeholders quickly. Communications would be clearer since the same message would be visible to all stakeholders. And it would be easier to ensure that messaging was managed by experts and leaders within the organization.

This is probably why 63% of respondents agreed that it would be advantageous, or extremely advantageous, to have a consolidated event management system to communicate between internal security stakeholders and external suppliers and partners during an incident.

SHOULD THERE BE MORE OVERSIGHT OF OPEN-SOURCE SOFTWARE?

In the USA, President Biden's 2021 executive order on improving the nation's security mandates an increase in scrutiny of open-source software in supply chains. Similar measures have been brought into place across the Western world. Our research shows that 72% of senior IT decision makers and cybersecurity leaders believe that greater government oversight of open-source software would make it more secure against cyber threats. 22% say that more government oversight would not make a difference, while 6% say that it would make using open-source software less safe.

It's clear that in the wake of far-reaching security incidents, and in a cybersecurity environment that can be challenging to monitor, many are attracted to the idea of increased regulatory supervision of open-source software.

There are, however, points to consider on both sides. The founding principle of open-source software is that anyone, anywhere, can use it and add to it. This strikes fear into the hearts of governments and businesses who don't like the idea of code with obscure origins, created perhaps by individuals or groups based in nations they regard with suspicion. Even setting aside matters of foreign policy, it's possible to wonder whether open-source coders are keeping security concerns in mind while led primarily by creative, academic or entrepreneurial motivations.

However, the very ubiquity of the open-source model in today's digital landscape demonstrates that there are many advantages to its decentralized approach. Usage of open-source software might not be formally supervised, but is scrutinized by the open-source community—and many would argue that this model is the most efficient.

Could regulators keep up with coders, or would governance create a bottleneck effect—or turn off the tap of this fount of coding creativity?

While incidents like Log4j cast long shadows, it may be worth questioning whether the software creation model is really to blame. It's certainly worth asking what effect increased security governance would have on the open-source software community.

LOOKING TO THE FUTURE

When major cybersecurity incidents are emerging via software supply chains, it's critical for organizations to find a way of alleviating their own security concerns when working with suppliers and partners. Organizations who produce or sell software feel the pressure from both sides: they have a responsibility towards their consumers, while depending on upstream partners to notify them of emerging security concerns. Many organizations find themselves in multiple positions within the network of their own and others' supply chains, adding to the challenges they face.

71% of organizations are calling for a tool that could inventory software libraries within their supply chain. They believe it would be useful to have greater visibility of software that might be impacted by a vulnerability.

In the event of a security incident in the software supply chain, organizations need to respond quickly to investigate the software they consume and produce, and alert partners and vendors as soon as possible. Clear, coordinated communication is essential in often sticky situations: for example, an organization might be holding their supplier accountable to patch a vulnerability while messaging their own customers, who see it as the organization's responsibility. 63% of organizations would find it helpful to have a consolidated secured event management system to communicate between internal security stakeholders and external partners during an incident.

At BlackBerry, the Product Security team uses an internally developed platform to determine the provenance and location of software that's in your products and systems. It's designed to discover and locate security issues in a matter of minutes and help defend against them. Currently, it's undergoing additional development to make it even more effective and easier to use. The platform also offers consolidated communication to manage security alerts, so that stakeholder messaging is efficiently coordinated. For more information on how BlackBerry's comprehensive, prevention-first, AI-driven cybersecurity solutions can help your business prepare for, prevent, detect and respond to cyber threats, please visit [BlackBerry.com](https://www.blackberry.com)

¹<https://www.newscientist.com/article/2301331-log4j-software-bug-is-severe-risk-to-the-entire-internet/>

 **BlackBerry** Intelligent Security. Everywhere.

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including over 215M vehicles. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security, endpoint management, encryption, and embedded systems. BlackBerry's vision is clear - to secure a connected future you can trust.

©2022 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY and EMBLEM Design are the trademarks or registered trademarks of BlackBerry Limited, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners. BlackBerry is not responsible for any third-party products or services.

For more information, visit [BlackBerry.com](https://www.blackberry.com) and follow [@BlackBerry](https://twitter.com/BlackBerry).

