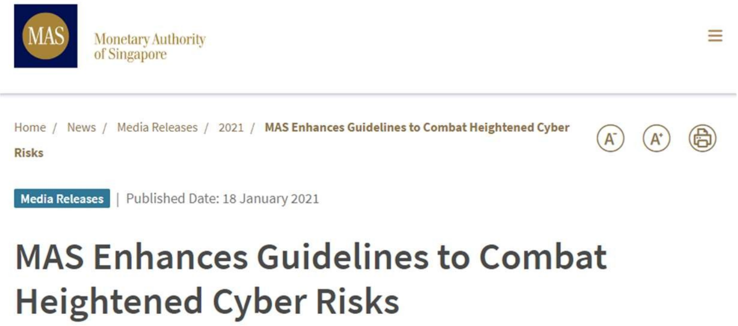
MAS Technology Risk Management Guidelines – What They Mean and How to Get Started

Summary of MAS Technology Risk Management (TRM) Guidelines

On 18th January 2021, MAS updated its cyber-risks guidelines in light of recent cyber-security incidents including the infamous SolarWinds breach.



MAS Monetary Authority of Singapore

Home / News / Media Releases / 2021 / MAS Enhances Guidelines to Combat Heightened Cyber Risks

Media Releases | Published Date: 18 January 2021

MAS Enhances Guidelines to Combat Heightened Cyber Risks

The enhanced guidelines detail best practices for managing technology risk by establishing a framework for technology risk governance and cyber resilience.

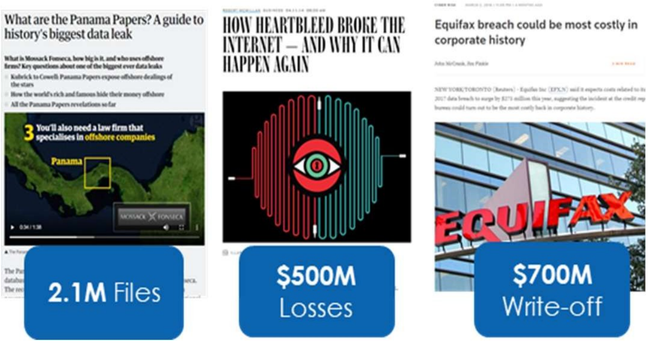
The framework encompasses risk identification, assessment and treatment, as well as monitoring, review and reporting to effectively manage vulnerabilities. At the same time, security-by-design should be incorporated into the application development cycle to ensure vulnerabilities are being identified and fixed early.

A key part of the TRM details the need for secure coding and application security testing. FIs can no longer pass on cyber-security liabilities to their vendors and need to establish a procedure and policy in place when using open-source software codes, and to keep track of reported vulnerabilities. The issue regarding open-source application code governance was also raised in the MAS advisory released on 14th November 2020. Given that the average application today is built on top of 250+ open-source components, not mitigating the risks associated with them can be catastrophic.

Background

The SolarWinds breach in December 2020 highlights the urgency and importance of securing the software supply chain. The affected application, Orion, is used by over 33,000 customers to manage their IT resources. Hackers breached Orion to install backdoors which were used to obtain information on the customer's IT systems, which then enabled the installation of additional malware and spyware.

When it comes to breaches arising due to insecure software supply chain, SolarWinds is not alone. Other notable data breaches due to insecure software supply chains include the Equifax breach, which exposed a third of all Americans' credit information and resulted in a 700M USD settlement, as well as the Panama Papers, which exposed more than 11.5 million documents of financial and legal records.


What are the Panama Papers? A guide to history's biggest data leak
2.1M Files
HOW HEARTBLEED BROKE THE INTERNET — AND WHY IT CAN HAPPEN AGAIN
$500M Losses
Equifax breach could be most costly in corporate history
EQUIFAX
$700M Write-off

How Do I Secure My Software Supply Chain?

To begin securing your software supply chain, you need to first understand the third-party software and open-source libraries in your systems and applications. Traditionally, we have been checking for vulnerabilities in the code we write but not so for security and legal issues on code that we depend on from third parties and open-source channels.

Up to 90% of codes used in applications are open source and imported by developers, which also means if they are not using a Software Composition Analysis (SCA) tool, up to 90% of the software supply chain is left vulnerable for exploitation. Using Scantist's SCA, you can easily identify the open-source libraries and third-party software and their associated vulnerabilities. Scantist's SCA also provides your team with smart, context-aware remediations and patches to remove and remediate these vulnerabilities.

Scantist proactively alerts your team of newly disclosed vulnerabilities. Over 500 new vulnerabilities are disclosed on the National Vulnerability Database in a week alone and you need to stay on top of those to stay secure. Scantist SCA does this for you by monitoring 33 million open-source and third-party artifacts round the clock, immediately alerting your organisation when there is a threat that needs attention.

Start Securing with Scantist

Protect yourself from widely known open-source vulnerabilities in 90% of all your code with an automated solution to detect and remedy vulnerabilities while increasing the productivity of your valuable developers – with no security expertise required.

Reach out to our team at Scantist to begin your security-by-design journey today! Email us at **contact@scantist.com**

Or better yet, try our solutions right away for free and get scanning within 15 minutes at **https://scantist.io**

For press-related enquiries, please contact **marketing@scantist.com**