Top Tips for Supply Chain Security During the COVID-19 Outbreak

The COVID-19 pandemic has placed immense pressure on the supply chain. With resources stretched and stability of the chain weakened, a primary concern for organisations is the availability of services.

COVID-19 has heightened supply chain information risk by:

- **affecting on-site security assessments**
- **forcing organisations to on-board new, unvetted suppliers in a hurry**
- **reducing suppliers' security capability due to staff illness and isolation.**

These ISF tips offer guidance on how to manage supply chain information risk during this time.

ISF Members can find related tools and research on supply chain security on ISF Live.

REASSESS YOUR SUPPLY CHAIN INFORMATION RISK APPETITE

To keep supply chains operational, organisations may need to tolerate greater information risks. Business risk appetite is likely to have changed in favour of availability over confidentiality or integrity. Agree and record changes to your organisation's risk appetite as it relates to the supply chain.

ADJUST SECURITY REQUIREMENTS FOR SUPPLIERS

Revisit minimum security requirements for suppliers, and apply amendments to existing and new contracts. The stringency of requirements may vary with each supplier, depending on their service, size and the information risk they present.

FIND ALTERNATIVES TO SELF AND ON-SITE ASSESSMENTS

Assume that existing security assessments are no longer accurate and on-site assessments are not viable. Look for online alternatives to verify that security controls have been correctly implemented. Request that suppliers share evidence electronically to maintain visibility of their current and ongoing security arrangements.

USE AUTOMATED SECURITY RATINGS TOOLS

While automated security ratings tools perform limited testing of internal systems, they can highlight early warning signs that a supplier's security standards are slipping. If your organisation has already deployed these tools, leverage them further to monitor the security status of suppliers.

MAKE USE OF OSINT

Consider using open source intelligence (OSINT), including tools and techniques such as vulnerability scanners and penetration testing, to monitor supplier security. You may also find information (e.g. on social media and hacker news sites) about a supplier's past security incidents as well as financial or market reports that indicate the supplier's priorities.

MAINTAIN CONTACT WITH SUPPLIERS

Identify points of contact with all critical suppliers and establish clear lines of communication. Develop a set of key questions and engage frequently to understand the impact of COVID-19 on a supplier's ability to operate securely and fulfil their contract. Remain vigilant and ensure your suppliers are aware of your in-house information security policies and procedures. Outsourcing does not diminish your legal responsibilities.

FIND OUT MORE

Discover more useful resources at **www.securityforum.org/covid-19/**

About the ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its members. Find out more at **www.securityforum.org**

Information Security Forum
@SecurityForum
info@securityforum.org

REFERENCE: ISF 20 04 01