Expert Views

Cybersecurity of the supply chain

SCOR
The Art & Science of Risk

September 2022

Introduction

The recent shocks, Covid-19 and Ukraine conflict, have highlighted how interdependent societies have become. Any disruption of the supply chain leads to a shortage of goods and an increase in prices of raw materials at a global scale. Digital technologies are powering the supply of goods and services worldwide making them a key asset for our collective productivity.

In the last 18 months, supply chain cyber-attacks have been a growing source of concern and have further demonstrated the ever-increasing interconnections among organizations.

However, a closer look reveals a pattern in the variety of situations where the supply chain has been targeted or used to perform cyber-attacks.

This paper presents two different risks:

- traditional suppliers being used to penetrate larger targets, and
- attacks leveraging software or IT services providers to attack their client base in-mass.

Methodologies and potential impacts differ in both situations, and we will aim to provide specific analysis and recommendations for each case.

Supply chain attacks are a growing source of concern

Supply chain attacks

+430% growth of supply chain attacks in 2021

"As enterprises have become better at hardening their environments, malicious attackers have turned to softer targets and have also found more creative ways to make their efforts difficult to detect and most likely to reach desirable targets," according to Crowdstrike.

1 out of 3

is the number of time suppliers are able to report how they were compromised[1].

Code is the weakness in 66% of the cases

In 66% of the incidents involving targeted assets, attackers focused on the suppliers' code in order to further compromise the targeted customers[1].

84%

of the IT security professionals panel believe that software supply chain attacks could become one of the biggest cyber threats to organizations like theirs within the next three years[2].

IT supply chain

59%

of organizations that suffered their first software supply chain attack did not have a response strategy[2].

6%

of the IT security professionals panel have vetted all new and existing suppliers for security purposes in the last 12 months[3].

203 dependencies on average

Today, the average software project has 203 dependencies. If a popular app includes one compromised dependency, every business that downloads from the vendor is compromised as well, so the number of victims can grow exponentially[3].

(1) ENISA Threat landscape for supply chain attacks
(2) CrowdStrike's Global Security Attitude Survey
(3) https://octoverse.github.com/#lets-look-back-at-the-code-and-communities-built-on-git-hub-this-year

Companies' supply chains have become more complex and more interconnected

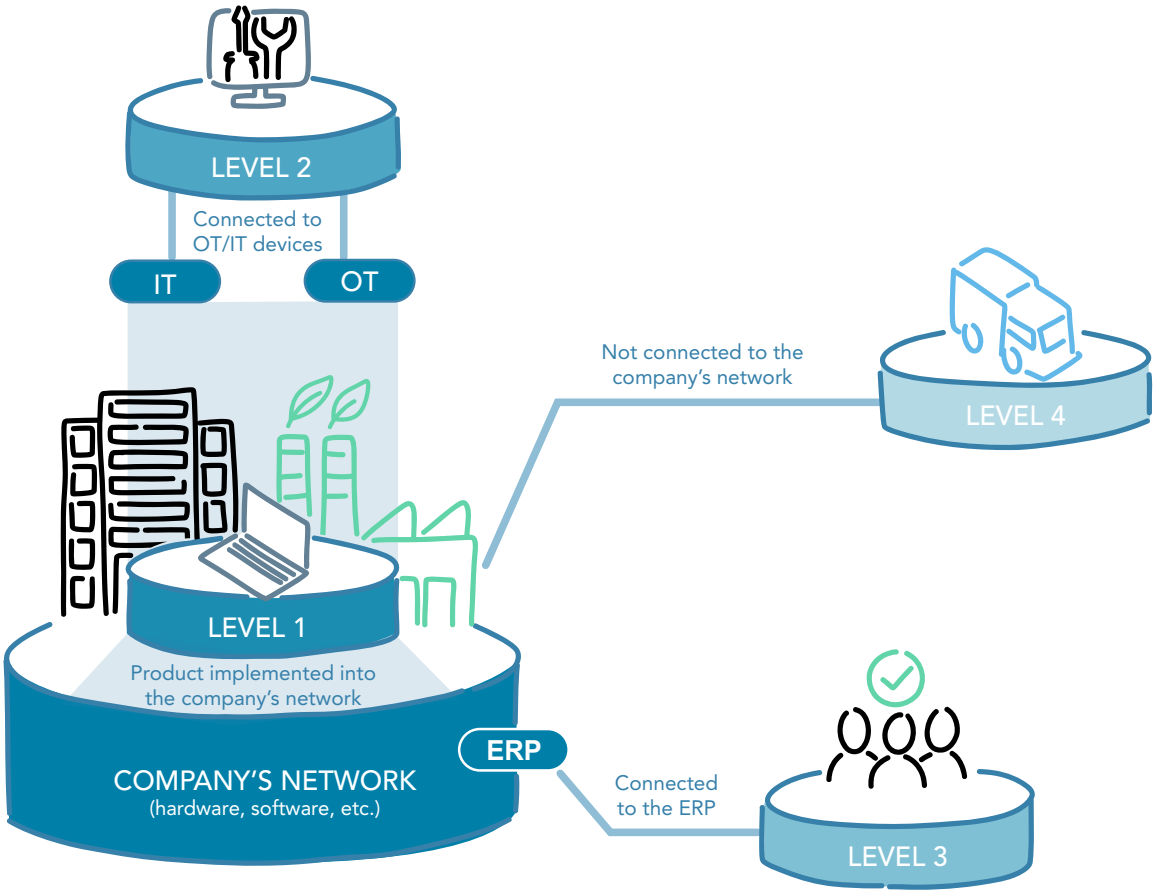
A diversity of suppliers' profiles

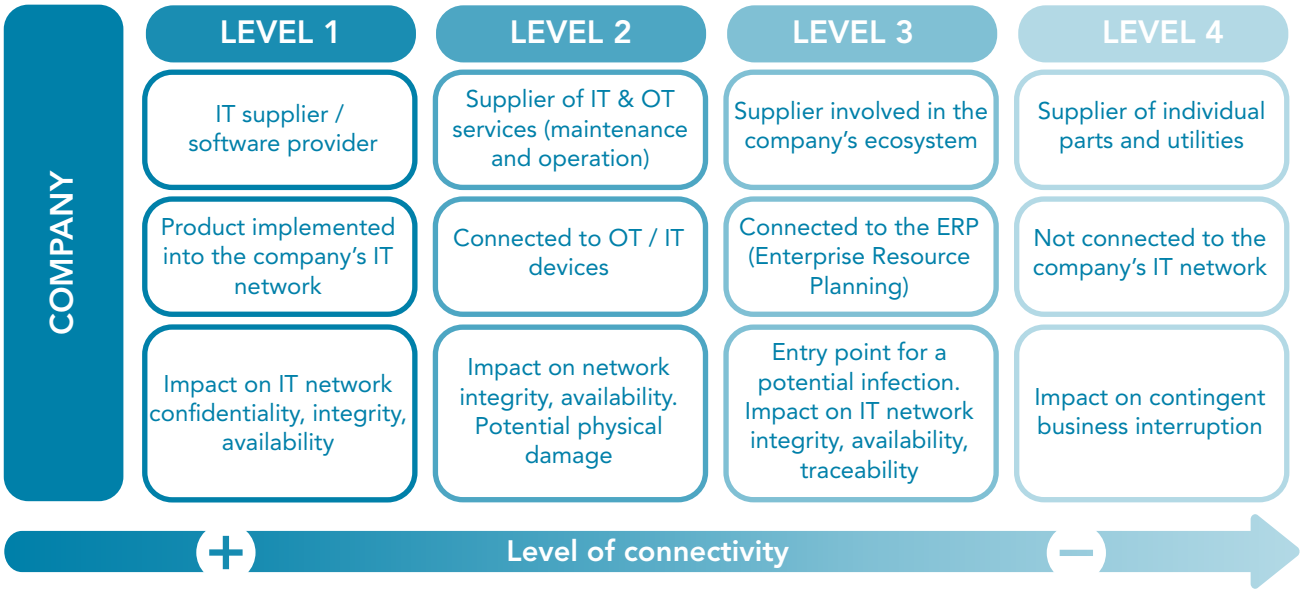
The traditional supply chain should be defined as a network between a company and its suppliers to produce and distribute products or services to final customers. This network includes different activities, people, entities, information, and resources.

The IT supply chain is a digital layer over the traditional one adding resources such as hardware, software, cloud or local storage, distribution mechanisms, and tracking or geolocation devices (RFID chips). These components are strongly interdependent and complex. For example, a software can include external libraries, opensource code, or code reused from another software. All these components are integrated to make businesses as efficient and reactive as possible.

The efficiency gains come at the cost of complexity. Disruptions of the IT supply chain cause cascading impacts on businesses, depending on how interconnected suppliers and clients are.

SCOR has designed a supply chain ecosystem classification (see below) according to the level of connectivity to prime contractors, as shown in the diagram below. This approach provides a way to assess how suppliers impact their clients and how cyber security measures can help mitigate the risk.





The physical and the digital layers of the supply chain are both parts of a whole, but each has different complexities and challenges to address.

What is a supply chain attack?

Not every cyber-attack is a supply chain attack.

For example, in 2021 T-Mobile faced a massive data breach during which hacker accessed almost 50 million customers' accounts data. This cyber-attack was not a supply chain attack even though attackers leveraged unprotected routers manufactured by an IT company – an IT supplier.

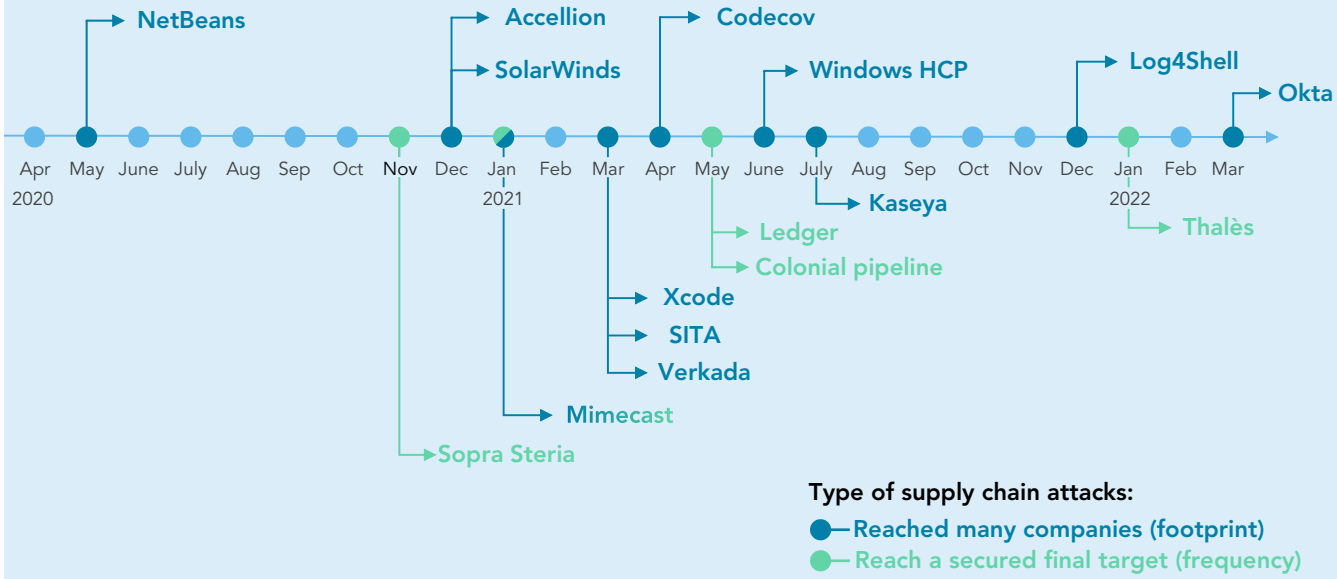
At first sight, it might be tempting to qualify most cyber-attacks as a supply chain attack because an attacker always leverages vulnerabilities in hardware/software developed by a third-party IT vendor. However, we believe a cyber incident should only be considered a supply chain attack when someone infiltrates an organization's system through an outside partner or provider with access to the organization's systems and data.

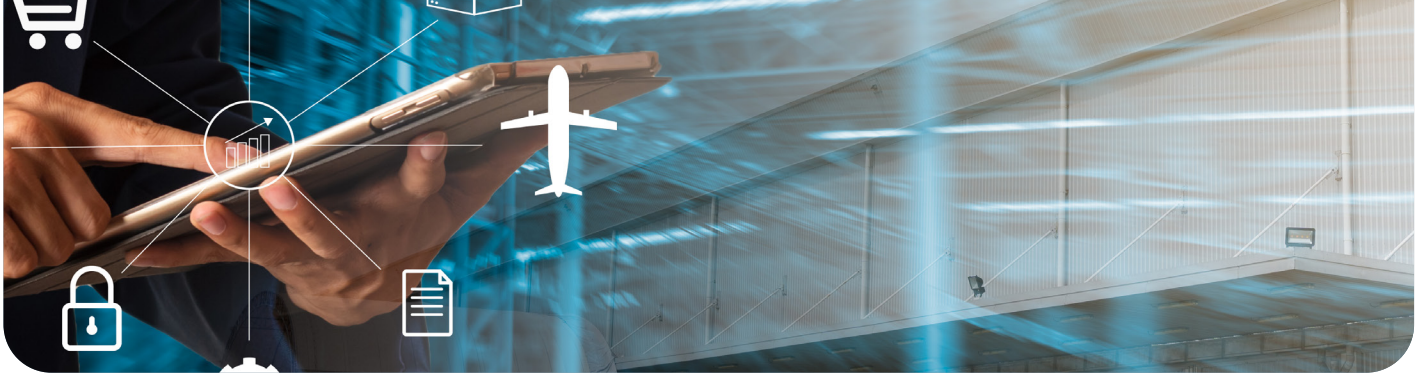
A significant increase but limited consequences so far

Supply chain attacks amplify impacts of cyber-attacks along two complementary axes as shown in the figure below:

- Increased footprint: by compromising a supplier, such as a popular software vendor, the attacker has the opportunity to impact many companies at once. Due to the concentrated IT market, one IT solution can be used as a common point of failure to reach many companies.
- Increased frequency: in the recent years, the "Just-in-time" business model has increased interconnections between suppliers and prime contractors. With this model, vendors who have less cyber-security measures in place than the company they serve are likely to become attackers' first target and be used as Trojan horses to breach secured companies that would have been difficult to attack directly.

The timeline of global supply chain attacks over the past two years gives a good overview of the acceleration of the number of the supply chain attacks:



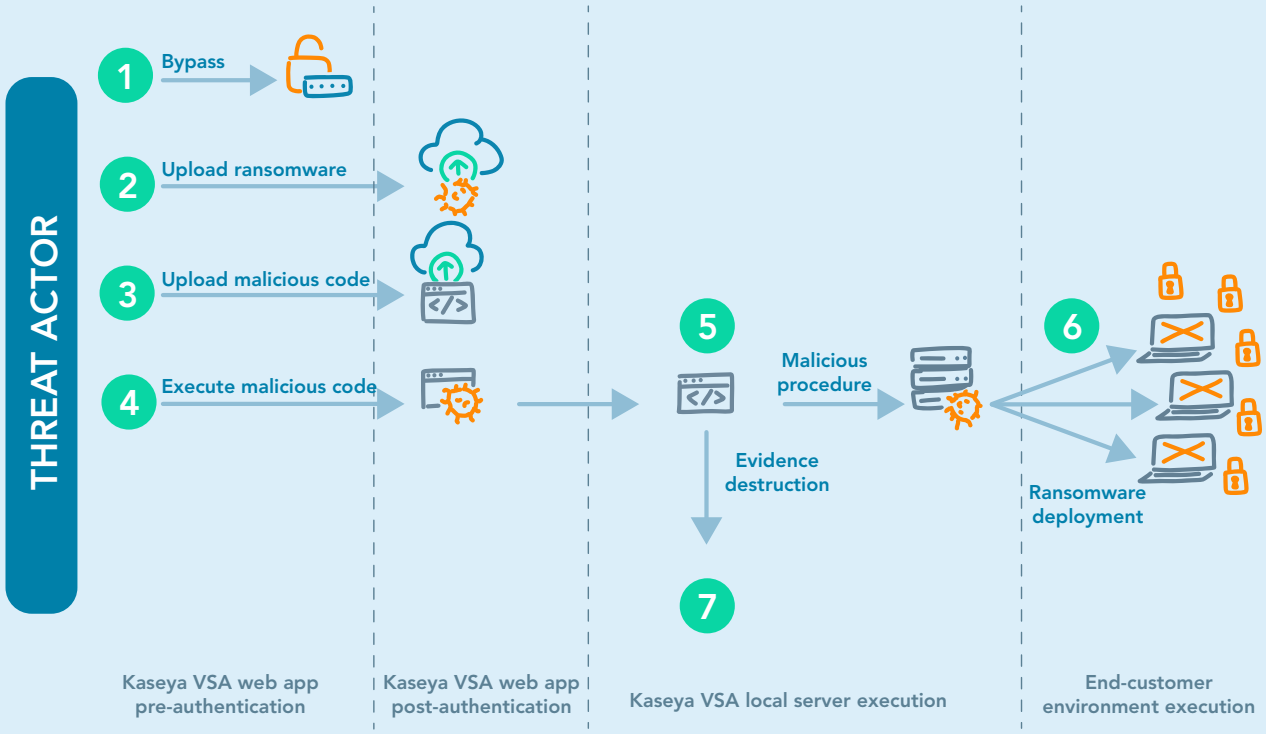


While supply chain cyber-attacks have increased in the recent years, the impacts remain limited. Indeed, performing IT Supply Chain attacks requires a very high level of preparation time, expertise, and funding. From a criminal hacker standpoint, this kind of sophisticated attack is only worth if the return on investment is sufficient.

As of now, most of the recent high-profile supply chain attacks have probably been performed for cyber espionage purposes and therefore having had limited economic impacts on victims. However, it is probable that criminal hackers may eventually reuse cyber spy's techniques to launch financially-motivated attacks that would have a much larger impact on companies and, in turn, on the (re)insurance market.

Focus on Kaseya cyber-attack:

In July 2021, Kaseya, a company that makes network monitoring and remote management software, experienced a ransomware attack. The attackers (criminal group REvil) injected malicious code into Kaseya's software development pipeline and exploited a zero-day security vulnerability in Kaseya's software (VSA), causing widespread supply-chain disruption. They were able to reach Kaseya's customers - mostly managed service providers responsible for everyday IT functions for small and medium businesses - as well as their network of 1,500 SMB clients. This demonstrates the potential that supply chain attacks have to simultaneously impact a large number of companies through a single point of entry.



The supply chain risk gets us into a pickle: critical control points to prioritize

The mapping and monitoring of the supply chain is a best practice that is already in place in many industries. The purpose is to collect information about suppliers and their own suppliers and create a map of the supply network. The mapping is updated in real-time to allow a continuous monitoring of the most critical suppliers.

However, this best practice is not always applied to the IT supply chain, despite the fact that it arguably deserves the same level of care and analysis as the classical supply chain. All the mapping and monitoring steps of the physical world are applicable to the digital world, thereby improving the visibility on direct and indirect IT suppliers. This visibility is critical for important tasks like maintenance that require privileged access to the IT and OT (Operational Technology) networks.

The 4.0 Industry is a concrete example of the convergence between the physical world and the digital world. The industrial cloud approach has opened industrial systems to external stakeholders encouraging companies to externalize many actions and services. As an example, several external vendors access OT networks for remote maintenance and operation purposes. Without cybersecurity, an attacker could penetrate the OT network and impact the industrial environment, potentially causing physical damages.

More precisely, the digital supply chain has a lot of entry points from the outside, for example:

- Patching: software patches are external components integrated in companies' systems. If they are implemented without being previously tested, they could embed malicious code and become a vector of compromise.

- Remote maintenance: as part as the Operational Technology (OT) infrastructure, attackers could gain access to systems through remote maintenance connections if they are poorly secured or if access credentials are too broadly shared.

- Outsourcing services: companies often outsource some IT services to third-party vendors who, in turn, may subcontract the operation to a local, smaller firm for cost optimization purposes. As a result, it is challenging for the company to control who effectively has access to its IT systems and ensure cybersecurity requirements are enforced down the supply chain line.

To sum up, companies must gain control over "external components" in their IT systems, people and software alike.

A fast-evolving environment where several initiatives are developing

Recent years have been an eye-opener for the market and initiatives have been launched or intensified to improve the cybersecurity of the supply chain.

The proof is in the pudding, let's have a look at industry initiatives

The improvement of supply chain cybersecurity can be initiated by an industry creating synergies between different market actors. For example, BoostAeroSpace(1), the European aeronautical digital platform, was created in 2011 to develop and implement a collaborative program for standardization and security of the Supply Chain of the European Aerospace and Defense industry(2). The main goal is to increase cyber protection levels for all aerospace suppliers, sharing best practices and expertise into the AirCyber® Community.

The cherry on the top: existing and upcoming regulations and standards will provide more guidance for supply chain exposure

Several recent or incoming regulations are mandating new measures to strengthen the suppliers' cybersecurity which should help mitigating some risks stemming from the supply chain. For example:

- GDPR Directive on Supply Chain Risk (draft documentation): The new directive is going to require the development of a robust third-party risk management program.

- NIS2 directive: The Network and Information Security (NIS) Directive is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. The proposed expansion of the Network and Information Security (NIS) scope covered by the NIS2 will require more entities and sectors to take measures.

- UN Cybersecurity Rules, Norms and Principles for Responsible State Behavior: The new UN rules set requirements to protect the information communications technology (ICT) supply chain.

- UK government: The UK government wants to boost the cyber security of the country's digital supply chains with a series of measures that could include mandating IT service providers to adhere to the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF).

- The NIST Cybersecurity Framework (2020): This framework includes "managing cybersecurity within the Supply Chain" that integrates supply chain risk management aspects throughout the other control families to help protect system components, products, and services that are part of critical systems and infrastructures.

- America's Supply Chains (February 2021): The order states that United States needs resilient, diverse and secure supply chains to ensure economic prosperity and national security.

- Improving the Nation's Cybersecurity - USA (May 2021): This covers a large range of cybersecurity mandates including supply chain risk requirements.

(1) https://boostaerospace.com/
(2) https://asd-europe.org/

A few rules to efficiently manage supply chain cyber risks

There is no magic recipe to guard against supply chain attacks because each one has its own dynamic and characteristics. But some essential cybersecurity measures are particularly useful to mitigate supply chain risks, as presented in the table below.

Cyber supply chain rules	How it improves the security level?
Perform in-depth supplier evaluation: include cyber clauses in contracts, assess the cyber posture with a questionnaire, test the cyber posture and cyber resilience of critical suppliers, ask for source code and application penetration tests, ensure the compliance with the relevant policies and regulation (NIST, SOC 2, ISO 27001/2), etc.	Ability to identify the criticality of an IT supplier and consider the possible IT failure of these suppliers
Hardening of the Active directory (AD): Regular AD audit and pen testing, specific roadmap about AD security, dedicated team for AD management, backup and recovery	Limits the attackers to compromise and take control of privileged accounts
Backups: follow the 3-2-1 backups rules that involve having at least three total copies of your data, two of which are local but on different mediums, and at least one copy off-site	Capability to restore quickly and properly data in the event of cyber incident
Patching management: strong processes and test of the patch's reliability before its implementation	Ability to ensure a quick response in the event of an emergency (e.g.: log4j vulnerability)
PAM (Privileged access management): use a PAM solution (ex: MFA, logging, principle of least privilege, etc.)	Risk mitigation of compromising privileged access or escalation
Remote maintenance management: identify remote users and accounts, implement analytics tools providing logs of remote actions	Minimization of direct connection to critical assets

Contextualizing the rules along SCOR classification scheme leads to the following applicability table:

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
	IT supplier / software provider	Supplier of IT & OT services (maintenance and operation)	Supplier involved in the company's ecosystem	Supplier of individual parts and utilities
In-depth supplier evaluation				
Hardening of Active directory				
Backups management				
Patch management				
Privileged access management				
Remote maintenance mgt.				

Cyber supply chain risk reveals market challenges

The traditional and IT supply chains will get more and more entangled to satisfy business efficiency and optimization, ultimately creating a global interconnected ecosystem. The related cyber exposure will grow both at individual company level and at global level.

At individual company level, the supply chain risk should be considered as a regular risk integrated in the cybersecurity management framework and follow best practices such as the classification of suppliers according to their level of connectivity as described above.

At the global level, cross-dependencies and single points of failure should be analyzed to monitor potential large-scale accumulation risks and cascading effects of supply chain attacks.

Building a sustainable and profitable cyber (re)insurance market is a collective journey where all stakeholders have a role to play. As a leading global reinsurer, SCOR is committed to supporting its clients as they navigate through the complex, fast-evolving cyber risk landscape.

This article is written by:

Alexia Morot
Cyber Underwriting Analyst
amorot@scor.com

Sébastien Héon
Deputy Chief Underwriting Officer Cyber Solutions
sheon@scor.com

For more information feel free to contact:

Cyber Solutions team

Didier Parsoire
Chief Underwriting Officer
Cyber Solutions
dparsoire@scor.com

Teodore Iazykoff
Cyber Risk Modeller
tiazykoff@scor.com

Olga Zeydina
Cyber Business Analyst
ozeydina@scor.com

Specialty Insurance team in London

Gillian Anderson
Global Head Cyber team
ganderson@scor.com

Simone Hardy
Underwriter
shardy@scor.com

Daniel Stewart
Underwriter
dstewart@scor.com

Specialty Insurance team in Paris

Béatrix de Boysson
Senior Underwriter
bdeboisson@scor.com

Karim Hamlat
Senior Underwriter
khamlat@scor.com

SCOR
The Art & Science of Risk

September 2022