Securing your Supply Chain with Threat-led Cyber Risk Ratings

About us

Orpheus is the only UK-government accredited cyber threat intelligence company providing cyber risk rating services. We are accredited to the highest level to provide threat intelligence for Critical National Infrastructure (CNI) organisations in the UK, and are trusted by major organisations worldwide to help them understand the cyber threats they face. Our powerful and award-winning technologies collect huge volumes of cyber risk data, which we analyse using Machine Learning and our highly skilled team to enable you to stop your cyber risks before they happen.

"Adversaries are increasingly exploiting supply chain vulnerabilities to steal America's intellectual property, corrupt our software, and surveil our critical infrastructure"1

US National Counterintelligence and Security Centre, 2018

Even if an organisation has excellent cyber security, there can be no guarantee that the same standards are applied by contractors and third party suppliers in the supply chain. Attackers will target the most vulnerable part of a supply chain to reach their intended victim"2

UK National Cyber Security Centre, 2018

Accredited by:

Introduction – why focus on suppliers?

A number of high-profile incidents have reaffirmed the way in which companies are increasingly held responsible for the security of their supply chain, not just their own network.

Most companies now rely on third parties to deliver some element of their business, and information about customers and other private data is usually spread among several organisations delivering services, Furthermore, From the attacker's perspective, as larger companies have improved their cyber security in recent years, adversaries have looked to find easier ways of compromising their targets. Cybercriminals and state actors are therefore increasingly looking to compromise these softer targets and exploit the relationship of trust they have with the larger entities, in what is called a **supply chain compromise**. This shift is driving the need for dedicated solutions to assess and mitigate this risk.

Factors from the target's side are also driving this shift. The increasingly interconnected nature of modern businesses mean that there are more opportunities to exploit privileged access and hop from one network to another. Similarly, an increasing uptake in outsourced services means more third parties hold your sensitive data.

Supply chain compromises take two main forms. The **peer-to-peer** or stepping stone model means compromising smaller or less-secure entities in a supply chain to get to an ultimate target; whereas the top-down model involves targeting a larger or more secure entity – typically a managed service provider or software developer/distributor – that can provide access to multiple targets at once.

The following case studies highlight the cyber risk associated with supply chain compromises, and the wide range of impacts they can create. While initially pioneered by sophisticated nation state groups, they are becoming accessible to a greater number of adversaries, such as financially-motivated cybercriminals. The increasing prevalence of these operations reinforces the importance of managing your supply chain cyber risk.

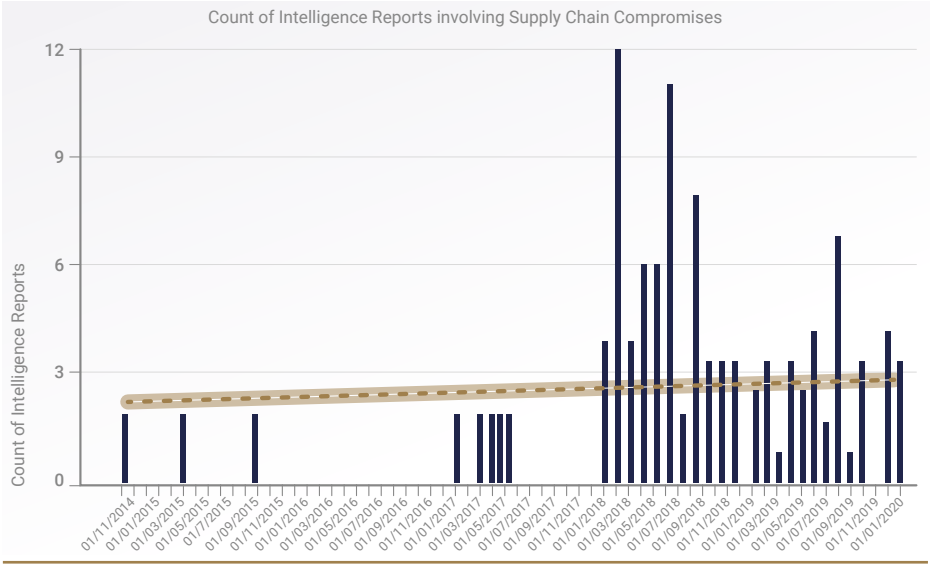


Figure 1: A graph showing the count of intelligence reports written by Orpheus' expert analysts over time highlights the increase in supply chain compromises since 2014.

> *"All organisations need to consider some element of Cyber Supply Chain Risk Management. If another party is involved in the delivery of a product or service to your organisation, then there will likely be an induced cyber security risk from that entity. Additionally, your organisation will transfer any untreated supply chain risk to your customers.*[3]
>
> **Australian Signals Directorate, 2019**

CASE STUDIES

NotPetya

In June 2017, a Russian state group illustrated the effectiveness of top-down supply chain operations to launch a wide-ranging destructive attack. The group compromised an update to M.E.Doc accounting software with wiper malware, which permanently deletes data and overwrites hard drives, disguised as ransomware. Although the operation primarily targeted Russia's geopolitical rival Ukraine, where M.E.Doc is most used, it was designed to spread to cause maximum disruption. The total damage was estimated at USD 10 billion, with the container ship operator Maersk suffering USD 300m in lost revenue alone.

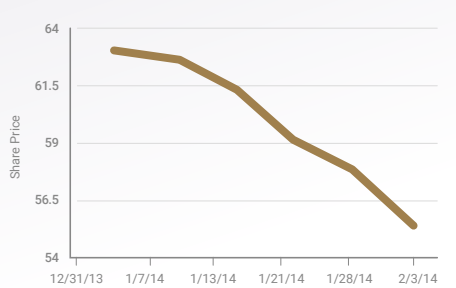
$300 million

Cost of NotPetya breach on Maersk

Sodinokibi

In August 2019, cybercriminals used the Sodinokibi ransomware variant to launch a mass ransomware attack on US dental practices. They initially compromised DDS Safe – a medical record storage solution – which in turn infected over 400 dental practices throughout the US. In addition to the disruption and downtime caused. Reports suggest that many practices were forced to pay the USD 5000 ransom to restore their access to the encrypted data..

Target's Share Price drops 11% post 2013 breach (USD)



Target

As far back as November 2013, cybercriminals identified supply chains as an attractive vulnerability and launched a peer-to-peer style supply chain operation against Target Corporation, initially compromising a weaker firm which supplied the US retailer. The group used phishing emails and keyloggers to steal VPN credentials from an air conditioning contractor to the US retailer, where the group moved laterally to infect point of sale (POS) terminals. The group stole payment card data for 41m customers, and contact information for 60 million more customers. Target settled a subsequent lawsuit for USD 18.5 million; its share price dropped 11%; and its CEO and CIO were fired.

AVIVORE

In October 2019, analysts at Context Information Security published their research on a new Chinese state actor they called AVIVORE. To target the European aerospace and aviation sectors AVIVORE would initially compromise smaller engineering and consultancy firms. It then pivoted from these companies to their clients, including larger multinationals, typically by exploiting a VPN connection between the two. The group, which mainly "lived off the land" through imitating legitimate activity, ultimately sought to steal valuable intellectual property.

APT10

Since 2009 or potentially earlier, the APT10 group has pursued targets related to Chinese foreign policy objectives and domestic industries. One of its ongoing campaigns, dubbed Cloud Hopper, has persistently targeted managed service providers (MSPs) and software companies such as IBM, Hewlett Packard and Norway-based Visma. These firms are not the ultimate targets, though, as APT10 instead seeks to exploit their connection to their clients to steal the latter's intellectual property.

"A series of high profile, very damaging attacks on companies has demonstrated that attackers have both the intent and ability to exploit vulnerabilities in supply chain security. This trend is real and growing. So, the need to act is clear" [4]

UK National Cyber Security Centre, 2018

MITIGATING THE RISKS

Despite this increasing threat, there remain practical solutions to mitigate the cyber risk associated with supply chains. The first element of the US NCSC's guidance is to establish a Cyber Supply Chain Risk Management (C-SCRM) program.

The UK NCSC advocates 12 principles to help you establish effective control and oversight of your supply chain, which are categorised in four separate stages:

1. Understand the risks
2. Establish control
3. Check your arrangements
4. Continuous improvement

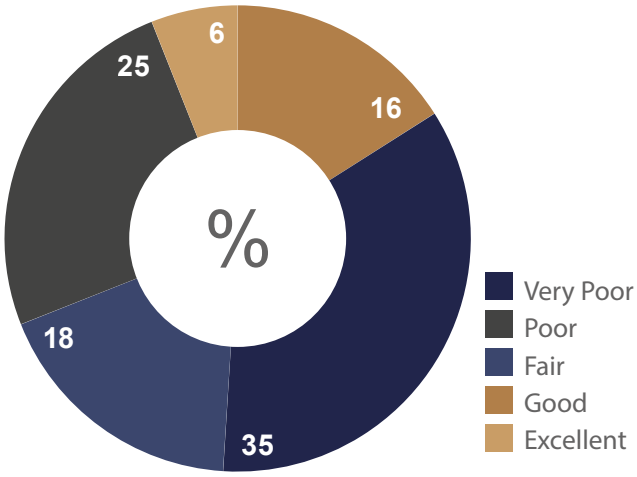
In addition to establishing a threat-led and risk-based approach, these principles highlight the importance of being able to continuously track and drive improvements within your supply chain. For example, when a company onboards a new supplier, they bring with them their own unique threat landscape. Alternatively, the emergence of new vulnerabilities on the networks of existing suppliers create new potential sources of cyber risk. As a result, companies are increasingly looking towards dedicated solutions that fulfil these key principles in helping them manage the cyber risk that derives from their supply chains.

Orpheus Cyber Risk Rating solutions help companies identify the different type and level of vulnerability and threat that different companies in a supply chain have. Crucially, it also helps companies – and their suppliers – identify, understand, and mitigate these threats and vulnerabilities, and make themselves less attractive from an attacker's perspective.

For example, a sample of more than 7,000 companies in our cyber risk rating tool showed that:

- **18% had internet-facing databases that criminals could look to steal from**, potentially including personal information
- **77% had had leaked emails**, which could be targeted in phishing or credential-stuffing attacks
- **39% of the companies had vulnerabilities on their public facing infrastructure.** Of that 39%, 52% had vulnerabilities that were of critical severity, meaning that they were more likely to be targeted by attackers.
- **16% of the companies lacked the most basic email authentication measure (SPF, Sender Policy Framework).** Only 8% had a more advanced measure (DMARC, Domain Messaging and Authentication, Reporting & Conformance) set up on email domains to prevent potential spoofing.

Breakdown of companies by risk rating category:



To better understand your supply chain cyber risk, or for a free Cyber Risk Rating for your company to discover how you compare with your competitors, please contact **contact@orpheus-cyber.com.**

[1] US National Counterintelligence and and Security Center (NCSC): "NCSC Launches National Supply Chain Integrity Month in April"
[2] UK National Cyber Security Centre (NCSC): "The Cyber Threat to UK Businesses"
[3] Australian Signals Directorate (ASD): "Cyber Supply Chain Risk Management Executive companion"
[4] UK National Cyber Security Centre (NCSC): "The Principles of Supply Chain Security"