Supply Chain CyberSecurity

Potential Threats and Rising to the Challenge

kaspersky.co.uk
www.securelist.com

kaspersky BRING ON THE FUTURE

Foreword

Recent extraordinary events including the COVID-19 pandemic, supply chain imbalances and Brexit have placed unprecedented challenges on those in the global supply chain. The magnitude of these events has witnessed activities in the supply chain being scrutinised through mainstream media like never before. The extent to which our lives are dependent on the smooth operation of the supply chain has rarely been so apparent, whether it be for luxury goods, every day essentials or critical medical supplies.

The reliance society has on the supply chain has undoubtedly attracted the attention of bad actors, those with intentions to disrupt and cause financial harm, however so motivated. The interconnectedness of the global supply chain makes for an attractive target for cyber criminals who could achieve great impact should their endeavours be allowed to spread easily amongst supply chain communities.

Sharp fluctuations in trade volumes have provided challenges and opportunities, but have certainly placed unwelcome additional strain on businesses. Many businesses are now in urgent need to recruit as demand for services continues to increase. An influx of new personnel inevitably introduces risk, from operational and safety training through to cyber hygiene training and maintaining secure systems.

The blockage of the Suez Canal in March 2021 was an unwelcome distraction, demonstrating not only the consequent operational challenges but how potentially fragile many supply chains are. The economic impact of the six-day blockage is estimated in the billions of dollars. As events played out over mainstream media, the enormity of a single pinch point became apparent.

While recognising recent stresses, one should not become complacent in the context of cyber risk. Many will have faced existential challenges through the last two years and will have turned focus and resources accordingly. Cyber risk however continues to flourish, the further into the limelight the supply chain is elevated, the more attractive a target it becomes.

As we emerge from the COVID-19 pandemic, actors in the global supply chain are encouraged to re-evaluate their cyber risk policies and satisfy themselves that sufficient resource is allocated to addressing this threat. Resilience in the face of cyber risk is critical in protecting not only your business and systems, but also those of your contractual partners.

One should not underestimate that cyber criminals are agile, focused and highly sophisticated, presenting a significant threat to businesses in the global supply chain.

Michael Yarwood
Managing Director Loss Prevention
TT Club

Contents

Introduction

Today's world is built on a web of digital connections, and each interaction is a potential opportunity for cybercriminals.

In 2021 cybercriminals became more sophisticated at exploiting organisational silos, remote workers, and the supply chain crisis to undermine the safety and security of critical systems. The pandemic has only accelerated the growing complexity and severity of cyberattacks.

Supply chain and third-party risks hit the headlines last year, with the SolarWinds and Colonial Pipeline attacks demonstrating how threat actors can target a vast number of organisations by breaching a single link in a supply chain.

> "Cyberattacks are becoming ever-more sophisticated, and collaboration is key to winning the battle against a very organised, well-funded group of adversaries. CISOs might think they are doing a great job protecting their organisation by building the proper controls and ecosystems, but their adversaries are sitting at a very different vantage point and focusing on the weakest link in their supply chain."
>
> **Jitender Arora,**
> **Chief Information Security Officer at Deloitte VL**

No matter how strong an organisation's security is, any weak link in a supply chain can bring a business to its knees. Our report found that companies of all sizes and sectors are failing to give CyberSecurity the attention it deserves in the current landscape. While just under three-quarters (72%) are prioritising CyberSecurity threats over pandemic recovery, a worrying number demonstrate CyberSecurity complacency for their own security, and that of their third-party supply chain.

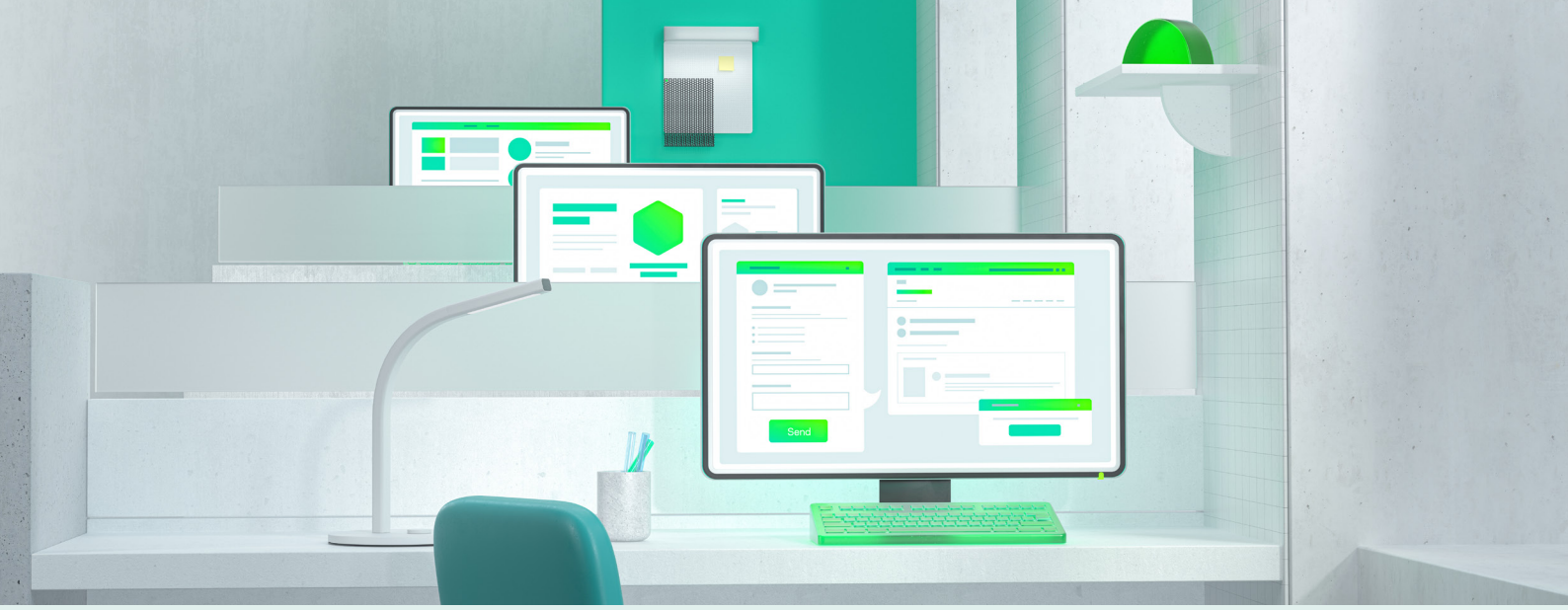
Companies both big and small cannot afford to be complacent. As organisations focus on overcoming supply chain-related challenges – such as unloading container ships and managing workforce shortages while minimising costs – cyberattackers have been leveraging a hyper-connected digital supply network to invent new attack vectors.

Our report highlights the need for businesses to scrutinise their suppliers' credentials as part of the standard due diligence and contracting process, or risk sleepwalking into a CyberSecurity disaster.

With the UK Government set to introduce proposals for legislation to increase supply chain IT security, pressure is mounting on businesses to ensure their suppliers are protected against cyberattacks.

At Kaspersky, we believe the pandemic and the knock-on effect on the supply chain has changed the cyberthreat landscape, and it is essential that organisations take steps to meet these new challenges. Companies should ensure they only share data with reliable third parties and extend their existing security requirements to suppliers.

This report aims to help technology suppliers, service providers, organisations, and security professionals understand the growing supply chain threat landscape. It also provides recommendations on securing and mitigating potential CyberSecurity breaches and that of third-party supply chains.



Methodology

During November and December 2021, Arlington Research surveyed 240 C-suite, middle managers (director level and above) and senior managers who are also sole or joint decision makers for CyberSecurity, IT and information security, across both SMEs (businesses with an annual revenue of less than £/€100m) and enterprises (businesses with an annual revenue of more than £/€100m). 150 interviews were completed in the UK (split 100 SMEs and 50 enterprises) and 90 interviews were conducted across Benelux (split 75 SMEs and 15 enterprises).

Key Findings

- 72% of organisations are concerned about CyberSecurity threats, more so than pandemic recovery (67%) and rising costs of raw materials (64%)
- Only a third of organisations (33%) strongly agree they have all the necessary resources and knowledge internally to respond to a CyberSecurity incident and only 35% of respondents 'strongly agree' that they 'have taken every possible step to mitigate third-party risks' to the organisation
- 16% of organisations deprioritised CyberSecurity during the supply chain crisis, despite 30% reporting a rise in attacks in the last 12 months
- Less than two fifths of decision-makers (39%) strongly agree that they trust their IT security provider(s) to help their organisation in the event of a CyberSecurity incident
- Only one fifth of organisations (20%) have third-party risk management insurance in place, while only 18% have cyber/business resilience insurance, despite 30% saying that they had experienced more cyber attacks over the last 12 months
- Two fifths (39%) of organisations are confident their business has adequate up-to-date hardware and software IT security protection
- Only two in five IT security decision makers strongly agree that they carefully vet the IT security of any new supplier or partner organisations before signing contracts, yet only 20% of organisations surveyed have a third-party risk management solution in place
- Three in five organisations agree they would never work with a business that has suffered a data breach, highlighting the importance of data security for future business opportunities

Supply Chain Risks

In any industry, if a supply chain's weak link is exploited a business can be brought to its knees.

A vulnerability in one place can significantly impact somewhere else, whether that's via compromised personal identity or payment credentials. Cyberattacks cause significant financial loss, intellectual property theft, psychological distress, disruption to services and assets, and risks to infrastructure. The impact can severely damage a company's reputation.

The National Cyber Security Centre (NCSC) says it has defended the UK from a record number of cyberattacks in the last year alone, including those targeted at supply chains. In November, the agency, which is a part of GCHQ, released its annual report showing that it dealt with an unprecedented 777 incidents over the last 12 months – up from 723 the previous year.

The NHS supply chain, for example, faces an ever-growing number of cyberthreats. Indeed, the health service's procurement process is as complex as it is sizeable. Cybercriminals will often take the easiest attack option, and that weak link can often be found in the supply chain.

"The NHS has a very extensive supply chain, so keeping it safe in the digital world is not an optional extra for our sector: it is a core requirement. If one of our suppliers is compromised and cannot deliver services, lives are put at risk, with potentially fatal outcomes."

"We protect against supply chain risk with the Data Security Protection Toolkit (DSPT), which demands baseline technical security standards and sets 10 security standards around people, process and technology to help guide trusts. The toolkit is an online self-assessment tool that allows health and social care organisations to ensure they are undertaking good data security and that personal information is handled correctly."

Paul Barnes,
Head of Operations and Engagement at NHSX

Even though almost three quarters (72%) of companies we surveyed state CyberSecurity threats are their number one concern, only a third (33%) strongly agree they have the necessary internal resources and knowledge to respond to a CyberSecurity incident, and just 35% of respondents 'strongly agree' they have taken every possible step to mitigate third-party risks in their organisation. Worryingly, less than two fifths of decision makers (39%) strongly agree that they trust their IT security provider(s) to help in the event of a CyberSecurity incident.

Cyber-insurance

In a world where cyberthreats are varied and constantly evolving, cyber-insurance can help organisations get back on their feet after an attack.

Yet our research found organisations are failing to take out insurance to protect their business in the event of a CyberSecurity breach, with only a fifth (20%) of companies reporting that they have third-party risk management insurance in place. The number was even lower (18%) when it comes to those with cyber/business resilience insurance.

"As well as helping businesses recover from an attack, partnering with a cyber-insurance company that can help identify any gaps in your security defences and is an extremely valuable way to eliminate risk, as well as mitigate it. This is important – otherwise, there's a danger of seeing cyber-insurance as a way of cushioning you from the effects of an attack, rather than using it as part of your risk assessment and management strategy".

David Emm
Principal Security Researcher,
Global Research & Analysis Team

Ticking time bomb: how current problems can affect future business

The pandemic first entered most organisations' radars two years ago, and supply chains were severely impacted.

As the virus became global, disruption became more widespread: logistics channels required rapid remodelling, suppliers became unable to meet contract terms and manufacturing plants closed due to component shortages.

Brexit also saw businesses divert attention away from CyberSecurity to focus on physical supply chain problems, such as HGV lorry driver shortages and logistics. In struggling to meet the ever-changing demands of the physical supply chain, have organisations taken their eye off the 'CyberSecurity ball' and risk sleep walking into potential disaster?

Once cybercriminals infiltrate an organisation, cybercriminals can cause disruption after disruption — it is a domino effect that affects suppliers, buyers and even consumers. And yet, our research also highlights a worrying level of CyberSecurity complacency amongst enterprises and SMEs alike - more than half (57%) of those we surveyed are concerned about the instability of supplier or partner organisations.

While the majority said that CyberSecurity has become a greater priority given the current supply chain crisis, concerningly, 16% have deprioritised CyberSecurity over the last 12 months.

Cyberattacks and data breaches can be highly injurious to an organisation in terms of damage to reputation, costs of remediation, lost business, and other expenses. This is borne out by our survey which found three in five organisations agree they would never work with a business that has suffered a data breach, highlighting the importance of data security for future business opportunities.

However, for a small number of organisations, the message that supply chain risk could impact their bottom line because they could be missing out on new business is not getting through, with 17% of organisations stating they did not expect to be questioned about their security credentials to win new business.

The National Cyber Security Centre (NCSC) recommends requiring suppliers to provide appropriate evidence of their security status and ability to meet their minimum security requirements throughout the various stages of the contract competition. For example, seeking basic assurances of their supplier's ability to meet legal and regulatory requirements, as a first gate, at initial contract advertisement, but requiring greater detail as the competition narrows to a choice of a few preferred bidders.

"If you have any kind of a trust relationship with an entity, you have third-party risk. The risk can come from a vendor, the company from which you rent your office, software suppliers, the app on your employees' phones, just to name a few."

"One of the biggest challenges businesses face when conducting a third-party risk assessment, is they tend to use a framework tailored to their individual needs.

We recommend getting all departments within your organisation involved in the process to help identify supply chain risk. For example, your financial team can check your vendor for certifications, money laundering and fraud, while your marketing and communications team can look for any adverse media. Occasionally you can request an initial penetration test (to evaluate the security level of an infrastructure) and if you want to go a step further you can conduct a full audit."

Vladimir Krupnov,
Threat Intelligence Lead at Revolut Bank

Seeing and preventing supply chain attacks

Lack of or poor security measures considerably increases the risk of a cyberattack taking place. A supply chain attack targets an organisation by infiltrating or attacking through a third-party vendor. If one of these entities has low CyberSecurity threat protection, it could become the point of entry into the whole supply chain. The risk can vary greatly and adds to the complexity of a company's threat surface.

The probable impact associated with cyberattacks varies for different actors within the supply chain. However, there are specific behaviours which can increase a business' vulnerability to cyberattack. These include, but are not limited to, weak overall internet or IT security measures, poor password policies, failure to keep software up to date, poor system monitoring and inadequate access controls. Lack of or poor security measures considerably increases the risk of a cyberattack taking place.

"Larger organisations can give small and medium enterprises, who are very good at what they do but not the best in terms of security, the offer of a helping hand, with advice and guidance to support their needs and improve the level of control. We often forget that we are talking about globalised attackers, who are very quiet and highly organised. We need to join forces and be a lot more organised on our side. One way we can really help our supply chain and third-party suppliers, especially SMEs, is to share our best practices and support them."

Jitender Arora,
Chief Information Security Officer at Deloitte VL

Supply chain cybercrime: more targeted, smarter

With some 90% of world trade transported by sea, coupled with the logistics challenges of COVID-19 and emerging new trends in cybercrime, the importance of cyber security in the supply chain has never been more critical.

The supply chain is inevitably an attractive target for hackers given that numerous actors in multiple jurisdictions will use common software applications, with the result that once the software has been compromised in one entity it may be possible to expose vulnerabilities across a range of businesses globally.

Awareness of the vulnerabilities across the maritime supply chain has been growing over recent years. The International Maritime Organization (IMO) recognised this and mandated **cyber risk management**[1] within the context of the existing **International Safety Management (ISM) Code**[2]. However, this necessary focus on the purely maritime aspects of cyber security should not be seen as a panacea. TT, in collaboration with UKP&I, **highlighted in 2018 the risks**[3] at the ship/port interface; the implications of cybercrime have only increased in the interim.

The last year alone has demonstrated multiple vulnerabilities that could each be exploited through a cyber-event. **Threats to the COVID-19 vaccine supply chain**[4] remain in the spotlight, as do the **impacts of the Suez Canal blockage**[5] and persisting pandemic risks.

What are supply chain cyber risks?

Cyber risks can be defined as the risk of loss or damage or disruption from failure of electronic systems and technological networks. In practice, we are talking of the illegitimate breach by hackers to access Information Technology (IT) or Operational Technology (OT) systems with the potential to disable controls, disrupt activities, or release, modify or destroy data.

In the maritime domain, such a cyber-attack might include radio frequency (RF) domains, meaning both global navigation satellite system (GNSS) and automatic identification system (AIS) jamming and spoofing are viable attack methods. This has significant implications for navigation and safe passage.

Similarly, Terminal Operating Systems used within the port infrastructure, for example cargo handling equipment, are equally vulnerable to potential breaches. Pandemic-induced dislocation and increased exposure from **remote working**[6] have only **heightened the risk of fraud**[7].

The latest threats

Cyber criminals are becoming **more sophisticated** in their approach. Ransomware attacks are more targeted than previously, cyber criminals are no longer taking a 'shot gun' approach and assessing who falls. The tools that cyber criminals have at their disposal are proliferating.

More targeted attacks, tailored to the target in terms of the demand are being made. Historically there may have been a simple request for US$500 in Bitcoin to re-establish access to systems. Today, the demand is aligned with the turnover of the company. Higher demands are assessed on the likely value of the denial of service, turnover and cash reserves to pay.

[1] https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx
[2] https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx
[3] https://www.ttclub.com/news-and-resources/publications/stoploss/stoploss-risk-focus---cyber/
[4] https://www.ttclub.com/news-and-resources/news/press-releases/2021/vaccine-supply-under-threat-from-theft-and-counterfeits/
[5] https://www.ttclub.com/news-and-resources/news/press-releases/2021/suez-canal-blockage-supply-chain-risks-assessed/
[6] https://www.ttclub.com/news-and-resources/publications/stoploss/stoploss-risk-focus---cyber/
[7] https://www.ttclub.com/news-and-resources/news/press-releases/2021/vaccine-supply-under-threat-from-theft-and-counterfeits/

Change of direction. Where a ransomware attack used to involve a simple denial of service, an attacker now might raise the stakes by adding in a threat not only to deny access, but to release or sell sensitive data on the dark web.

Third party service providers contracted to manage cyber security have themselves become a target for cyber criminals. According to a recent Kaspersky survey, 28% of managed service providers (MSPs) reported that a massive supply chain attack on an MSP software provider, revealed in December 2020, had affected their organization in some way. The breach also had a wider impact on the majority of MSPs: overall, 72% of providers took action in response to the attack, even though they were not affected. This and other security incidents targeting the IT service ecosystem highlight the need for increased CyberSecurity across MSPs, including both internal protection and specialized security services for customers.

Apart from the obvious motivation of financial gain, there are well-documented instances where the innate attributes of the global supply chain – the systems and processes to facilitate trade across national borders – have been exploited to carry out illicit trades, primarily around narcotics and people trafficking.

The general public in most, if not all, countries around the world in recent months have had their awareness of the global supply chain heightened, whether through media on their screens or gaps on shop shelves. Many will be aware also of the recent ransomware attack involving the US fuel supplier, Colonial Pipeline[8], which effectively shut down their supply system.

Such public awareness is compounded in the global supply chain by the impact on national economies. As the feasibility of more damaging cyber activities increase – whether initiated by criminal or more sinister state actors – all stakeholders involved must prepare for the inevitable and build resilience to the evolving cyber threats.

The reality is that all businesses are susceptible to a Colonial Pipeline event, more than likely resulting from an employee failing to spot a phishing email and launching a malicious link

Peregrine Storrs-Fox
Risk Management Director, TT Club

[8] https://www.ttclub.com/news-and-resources/news/press-releases/2021/suez-canal-blockage-supply-chain-risks-assessed/

Checklist – what can you do to protect your business?

› **Identify your suppliers**
The most important – and often overlooked step – for any organisation. Make an inventory of whom you buy products and services from and where your organisation sits in the supply chain, so you can start drawing a map of potential risks.

› **Identify what needs to be protected**
Being attacked through a supply chain typically means that a service or program that you have used for some time has been compromised. Every single business device with Internet access must be protected, including computers, servers, mobile phones, and so on. While the network should be protected from opportunistic, easy-to-monetise cybercrime attacks, it's also vital to deploy technology that will alert you to the early signs of intrusion by threat actors that wish to compromise the system for purposes of cyber-espionage.

› **Identify the risk to your organisation**
Consider potential vulnerabilities that could provide an attacker with an entry-point into the organisation. This should encompass policy and processes as well as technology. Moreover, this must include things over which you have no direct control – products and services provided by third parties. This might be applications, code running on your systems and remote access a third party might have to the network.

› **Evaluate suppliers' processes and security**
You should carry out a thorough audit evaluating your suppliers CyberSecurity credentials, risk management plans and whether or not they scrutinise their own suppliers in the same way. This should give you a good indicator of risk and what processes should be carefully managed.

› **Take action**
Develop a robust incident response plan, with a well-prepared – and dedicated –team and clear objectives. This should also include a critical risk mitigation steps in case an attack were to strike.

› **Use the tools at your disposal**
Cyber Essentials, for example, is a simple but effective government-backed scheme that aims to help businesses of any size protect themselves against a whole range of cyberattacks. The IASME consortium – NCSC's Cyber Essentials Partner – can help you to get certified. A Cyber Essentials readiness toolkit is also available, helping you draw up a personal action plan and move towards meeting the key requirements.

Putting risk management into action safely

Our survey highlights that it is critical for organisations to build robust programmes for managing both known and unknown supply chain risks. Leaders should also recognise that risk management is not merely about setting up processes and governance models, but also entails shifts in culture and mind-sets, helping suppliers further down the supply chain to adopt robust levels of controls.

By employing these approaches, organisations increase their chances of minimising supply chain disruptions and crises, while capturing the full value of their supply chain strategies.

To respond to supply chain risk challenges, and provide help to companies requiring specific CyberSecurity protection, Kaspersky specialists have developed Interactive Protection Simulation (KIPS), an exercise that places business decision makers and IT security teams from corporations and government departments into a simulated business environment facing a series of unexpected cyberthreats, while trying to maximise profit and maintain confidence.

The idea is to build a cyber-defence strategy by making choices from amongst the best proactive and reactive controls available. Every reaction made by the teams to the unfolding events changes the way the scenario plays out, and ultimately how much profit the company makes or fails to make. Balancing engineering, business, and security priorities against the cost of a realistic cyberattack, the teams analyse data and make strategic decisions based on uncertain information and limited resources. If that sounds realistic, it should do, because each of the scenarios is based on real-life events.

To learn more about Kaspersky Interactive Protection Simulation, please visit:
Kaspersky Expert Security

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Technologies at glance: www.kaspersky.com/TechnoWiki
Threat Intelligence Portal: opentip.kaspersky.com
Awards and recognitions: media.kaspersky.com/en/awards
www.kaspersky.com/fraudprevention

www.kaspersky.co.uk