Untangling the supply web

Managing third-party and supply chain risk

Risk Universe
by RiskBusiness

All organisations, no matter how small and uncomplicated, are impacted by third party/supply-chain, or "Nth-party" risk as it is also known. In this report, we take a look at some recent examples of risk events which have impacted the financial services supply chain in particular and put forward some workable solutions for minimising the impact of this risk.

SolarWinds

The SolarWinds hack in 2020 was one of the biggest cyber hacks of the 21st century. It was a particularly significant event because SolarWinds supplies online system management tools for hundreds of thousands of companies around the globe.

What happened at SolarWinds?

Hackers gained access to the SolarWinds network and planted malicious code (now known as "Sunburst") into its Orion network management system. More than 30,000 organisations were using SolarWinds' Orion product to manage their networks at the time, including several US Government agencies. The hidden malicious code planted by hackers meant that when users were sent a routine Orion software update, they were unknowingly installing the malware into their own systems. More than 18,000 SolarWinds users are understood to have installed the malicious updates. This included large, global tech firms such as Microsoft and Intel and cyber security firms such as FireEye - which was the first company to detect the hack.

What data was compromised?

Hackers were able to gain access to sensitive data held by government agencies including, the US Treasury, the Pentagon, the Department of Homeland Security, the State Department, the Department of Energy and the National Nuclear Security Administration (NNSA).

It is unclear exactly how much data was compromised or the exact objectives of the attack. It is believed the breach may have begun as far back as September 2019 and was not detected until December 2020, giving the hackers free reign for over a year. The UK and US governments have both blamed the attack on Russia's SVR (The Foreign Intelligence Service of the Russian Federation) agency. Increasing numbers of companies are discovering that they were victims of the attack - more than eight months after it was uncovered - including computer-aided design software manufacturer Autodesk, who recently reported it in their latest quarterly results. The true impact of the event is still unfolding and it will be some time before we know the full implications.

Akamai Technologies
Akamai, one of the world's largest providers of content delivery networks, suffered an outage in July this year, impacting major banking websites including HSBC, Barclays, Lloyds, Sainsbury's Bank, Tesco Bank and several gaming and retail sites. The outage lasted just over an hour and was caused by a configuration update which triggered a DNS (domain name system) bug.

The DNS is what links a website with its IP address. A DNS bug causes a glitch in this process, essentially preventing internet access for the affected website. Content delivery networks (one of the services provided by Akamai) are physical network servers which are geographically spread to optimise website performance by ensuring close proximity for end users. In basic terms, it is a network of servers spaced apart so that everyone who wants to access a website can do so.

> A DNS bug causes a glitch in this process, essentially preventing internet access for the affected website

Was the Akamai outage the result of a hack?
No. According to Akamai, the outage was caused by a software configuration update, rather than a cyber attack.

Capital One/Amazon Web Services hack
In July 2019, Capital One confirmed it had fallen victim to a data hack. An ex-Amazon employee, Paige Thompson, is accused of creating a software program to exploit a common glitch in the firewall of the web app used by Amazon Web Service (AWS) customers. More than 100 million Capital One customers were affected by the hack, plus a confirmed eight other companies using the service. It is understood that as many as 30 companies in total may actually have been targeted.

Thompson is believed to have downloaded the details from 106 million Capital One credit card applications, which included information such as social security numbers, bank account details, birth dates and addresses. It is still unclear what happened to the data after it was downloaded. Thompson is also accused of using AWS customers' cloud computing abilities to set up cryptocurrency mining operations.

AWS were also back in the news at the beginning of September 2021 when a hardware device failed, leading to system outages for several banks, brokerages and airlines in Japan for almost an entire day.

> Capital One was fined US$80m by US regulators for failing to protect customer data

Sita/Singapore Airlines
Sita supplies IT systems to the air transport industry and suffered a data breach earlier this year. The breach impacted several of its customers who used Sita's passenger service system, which shares frequent flyer data with other airlines within the same airline alliance. Singapore Airlines was one of the firms affected by the breach. Though it was not a direct customer of Sita, it had shared data with another firm within the Star Alliance of airlines, which did use the service.

The above examples demonstrate how wide-reaching a supply chain incident can be. Capital One was fined US$80m by US regulators for failing to protect customer data - even though it was the AWS system that the hacker gained access through. In the Akamai example, cyber security wasn't the issue, so due diligence checks in this area would not have prevented this event from happening. And the SolarWinds incident proves there are some third-party risks that we are completely oblivious to, causing untold damage and occurring as we speak.

Mitigating supply chain risk

Supply chain due diligence - KYSC, Know Your Supply Chain
Supply chain and vendor risk isn't just about cyber crime and technical outages; it's also about how your suppliers conduct themselves in a world that increasingly prioritises corporate ethics, both from a consumer and regulatory perspective. Corporate social responsibility and ESG (environmental, social and governance) issues are therefore now a huge part of risk management. Selecting vendors who demonstrate due diligence in this area, and asking them to provide evidence of this, could help avoid a PR disaster by association further down the line.

KYC (know-your-customer) checks are already a well-established part of the risk management process and know-your-supply-chain checks should receive the same level of focus. Regulation in this area is becoming increasingly broad, with the European Union having made moves towards a mandate on supply chain due diligence. The proposed EU *Directive on Mandatory Human Rights, Environmental and Good Governance Due Diligence* focusses on forcing companies to conduct due diligence in their supply chains and also outlines the legal right for individuals and company stakeholders to hold companies accountable for non-compliance.

Pressure testing your scenario analysis
If recent events have taught us anything, it's that anything can happen. With the last 18 months providing a perfect storm in terms of supply-chain risk (COVID-19, Suez canal blockage, Brexit, a Taliban government in Afghanistan), firms need to look at how they categorise their risks in terms of their likelihood and impact in the current context. One of the silver linings of the COVID-19 pandemic is that we now have real-time data on how an event of this magnitude impacts third-party risk in banking. Firms can now use this knowledge to create a mitigation plan

that fits the specific needs of the organisation.

Take a closer look at contracts and service level agreements (SLAs)

Now is the time to take another look at any third-party contracts you have in place to see what measures are available if the promised level of service is not delivered. The COVID-19 pandemic exposed grey areas in many contracts. For example, thousands of companies believed they would have insurance cover for loss of earnings due to the pandemic, but this often wasn't the case. With the potential for recurring waves in COVID-19 cases and additional lockdowns around the globe, it is worthwhile checking what measures your contractors have in place to mitigate the risks associated with this.

Don't stop at third party

The terms "supply chain" and "third party" are perhaps out of date in today's business environment. The interconnected nature of business means companies are often connected through a complex network, or "supply web" rather than a supply chain. This means that mitigating risk in this area shouldn't stop at your third-party suppliers. You may not have an account with AWS for example, but does your cloud services provider? How might they be impacted in the event of a breach? What cyber security measures do they have in place? Cases like the Singapore Airlines and Sita example above demonstrate how important it is to consider all business entities linked to the firm, especially those you choose to share data with. A survey of 1,800 businesses conducted by Refinitiv in February 2020 found that 60% of respondents were not fully monitoring third-party suppliers for on-going risks. 62% said they did not know how many third parties they engage are outsourcing work to others. 53% said they would report a third-party breach internally and only 16% would report it externally, demonstrating just how quickly the firm's perspective on this type of risk can become murky.

> 62% said they did not know how many third parties they engage are outsourcing work to others

Operational resilience

Managing third-party risk is a key component of operational resilience; a concept which has become a principal focus for regulators over the past 18 months. Earlier this year, the Basel Committee on Banking Supervision (BCBS) released its Principles for Operational Resilience, which outlines seven key principles for financial institutions to apply:

1. Governance
2. Operational risk management
3. Business continuity planning and testing
4. Mapping interconnections and interdependencies
5. Third-party dependency management
6. Incident management
7. ICT including cyber security

Principles 4, 5, 6 and 7 all touch on the subject of supply-chain risk:

Banks should carry out a risk assessment before entering into a third-party agreement

Mapping interconnections and interdependencies

According to the Basel guidelines, once critical operations[1] within the firm have been identified, banks should then map any interconnections and interdependencies that they rely upon to function, including all relevant people, technology, processes, information and facilities.

Third-party dependency management

Banks should carry out a risk assessment before entering into a third-party agreement and should verify whether the third party has "at least equivalent level of operational resilience to safeguard the bank's critical operations in both normal circumstances and in the event of disruption." The guidance also recommends looking at other viable alternatives to third-party arrangements should a disruption occur, such as bringing those operations back in-house.

Incident management

An inventory of incident response and recovery resources should be maintained, including both third-party and internal resources. Incident management should include the entire life cycle of incidents, including severity classification, response and recovery procedures, communication plans for reporting incidents to all stakeholders and lessons learned.

Incident management procedures should be reviewed, tested and updated regularly and root causes should be identified to help avoid recurrence.

ICT including cyber security

A bank's ICT policy should be fully documented and include governance and oversight responsibilities, risk ownership and any ICT security measures currently in place. Cyber security controls, incident response and business continuity and disaster recovery plans should be reviewed and monitored periodically.
Critical ICT assets must be identified and their security measures tailored to protect those assets which are most significant to the bank's critical operations, including plans to safeguard critical data in the case of a cyber security risk event.

Supply chain security vs other supply chain risks: avoiding silos

Third party, Nth party, or supply chain risk - whatever your firm chooses to call it - is

a complex and almost never-ending web of potential issues for the firm. This network of risks simply cannot be managed by the risk management function alone. One obvious area that should be covered by specialists is supply chain cybersecurity, which should fall under the remit of the chief information security officer (CISO). A joint report published by ComputerWeekly.com and Tech Target, *The CISO's Guide to Supply Chain Cybersecurity*, discusses the changing role of the CISO: "The reliance on third-party providers has created new demands on cyber security defences, adding complexity to the responsibilities of the chief information security officer (CISO)," it says. "Now more than ever, CISOs need to be more directly engaged with the broader risk management function or even take on a risk management leadership role. Recent high-profile supply chain security breaches have attracted the attention of CEOs and their boards. CISOs have found themselves needing to leverage both technology and leadership skills to effectively communicate the potential impact of supply chain attacks to the leadership team, and to drive executive buy-ins on solutions or mitigation efforts."

Good communication between departments and business functions is absolutely critical. The audit and compliance functions are well placed to help break down silos within the firm because they have unique access across all areas of the business. IT teams also have a responsibility to ensure they communicate in a manner that does not alienate those in non-IT functions. Speaking in jargon and losing patience with individuals who do not have a technical background only serves to widen the communication gap between departments and quite probably will deter people from raising the alarm when a potential breach has occurred, especially one due to human error. Providing regular training on cyber security protocols, having an open-door policy and ensuring a direct line of contact between senior leadership and every level of the business down to entry level, is essential. Every member of staff who is responsible for connecting with a third party should understand the company protocol for managing third parties and should be a part of the risk assessment process.

Further reading:

The CISO’s guide to supply chain cybersecurity: https://media.bitpipe.com/io_10x/io_102267/item_1306461/CISOs_guide_to_supply_chain_cybersecurity.pdf

The real risks: hidden threats within third-party relationships: https://www.refinitiv.com/content/dam/marketing/en_us/documents/reports/hidden-threats-within-third-party-relationships-2020.pdf

Operational resilience, Basel guidelines summary: https://riskbusiness.com/blog/operational-resilience-basel-guidelines-summary/

Proposed EU directive on Human Rights, Environmental and Good Governance Due Diligence: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0073_EN.html

ESG regulation: what you need to know: https://riskbusiness.com/blog/esg-regulation-what-you-need-to-know/

Know Your Supply Chain: Recordkeeping for Due Diligence and Compliance: https://www.lexology.com/library/detail.aspx?g=0c55f354-d7af-4a3c-bbd7-53f8d70751d5

About Risk Universe

Risk Universe by RiskBusiness provides in-depth analysis, reviews and research on areas of interest within the broader governance, risk, audit and compliance landscape, designed to provide proactive, 360° intelligence for informed decision making across the enterprise.

Contacts

Mike Finlay, Chief Executive:
mike.finlay@riskbusiness.com

Carrie Cook, Editor:
carrie.cook@riskbusiness.com

General enquiries:
info@riskbusiness.com

www.riskuniverse.com

Risk Universe by RiskBusiness

www.riskbusiness.com