TECHNOLOGY

Code red: the growing threat from supply chain attacks

iStockphoto/ Bahtiar Gil

Solarwinds was hit by a cyber attack that affected other businesses in its supply chain

With complex third-party cyber attacks exposing vulnerabilities in the digital supply chain, businesses need to be increasingly vigilant to protect both themselves and their customers

Alex Wright

Global supply chains have been exposed to unprecedented risk in recent years. A host of issues, ranging from Brexit and the Suez Canal blockage to the Covid-19 crisis and, most recently, the war in Ukraine, have all caused huge disruption.

But supply chain risk is not limited to the physical sphere. As businesses have grown exponentially thanks to increased digitalisation and reliance on third-party digital products, they have left themselves exposed to a growing cyber threat.

Supply chain attacks are when a company's data is compromised via the hacking of a third-party supplier with legitimate access to its customers' systems. Hackers can insert malicious code into trusted hardware or software at the source, compromising the data of its customers – and then their customers – in an onward chain.

One of the most devastating examples of this is the 2020 SolarWinds incident, referred to by Microsoft president Brad Smith as the "largest and most sophisticated attack ever".

In late 2019, the major US IT firm was targeted by hackers – later identified as originating in Russia – who used malicious code to gain access to the sensitive data of many of SolarWinds' clients, including technology giants Microsoft and Cisco, and the US Department of Homeland Security. In March 2020, SolarWinds began unwittingly sent out software updates to its customers that included the hacked code, which enabled the hackers to access their IT systems and data too.

The breach went undetected for months, with some victims not knowing whether they had been hacked at all. The full extent of the attack is yet to be determined, meaning it could take years to fully secure all the systems affected.

As companies have accelerated their digitalisation strategies to continue operating and to support their staff remotely during the pandemic, so they have become more dependent on third-party software and tech. This, in turn, has increased firms' attack surface exposure and points of vulnerability.

Supply chain attacks often start due to a mismanagement of critical access points. Known weaknesses in IT management platforms are then exploited, as evidenced by Log4Shell, a critical vulnerability in the logging tool Log4j that is used by millions of computers worldwide.

Hackers target victims through the key communication channels and software of third-party suppliers to gain access to their customers. A favoured attack method is through hijacked software updates – as in the SolarWinds case – which accounts for 60% of software supply chain attacks and disclosures, according to research by US think tank The Atlantic Council.

"Over the past few years, there has been an increase in next-generation supply chain attacks," says Ilkka Turunen, field chief technology officer at supply chain security firm Sonatype. "These direct attacks can involve, for example, malicious actors injecting new vulnerabilities into open source projects."

To combat the threat from these attacks, companies must have full visibility of all of their third-party relationships and dependencies. That means reducing the number of third-party providers they use, wherever possible, so there are fewer entities they have to monitor. Of course, this does not guarantee the integrity of their products.

"Regardless of the vendor's reputation, the product itself might have security gaps," says Heinrich Smit, who is deputy chief information security officer at cybersecurity specialists Semperis.

"When working with newer companies, be sure that you can view the company's product controls. Independent code reviews and application vulnerability reports are also very helpful because they evaluate a product inside the code and in situ from a penetrability perspective."

When assessing third-party suppliers, companies must ensure that they are thoroughly vetted and that their security practices meet the required standards. They also need to put in place a contract with the appropriate clauses to ensure they comply with the necessary regulatory and legislative privacy and security requirements.

Firms also need to analyse emerging third-party risks, as well as monitoring for suspicious activities on their systems and network. They should also only give network and systems access to those third-party vendors and apps that require it to perform their duties, and identify and monitor all access points.

Patching should be carried out on an ongoing basis, by ranking and scheduling updates in order of importance. In addition, organisations should regularly backup their systems to maintain their data.

This is in addition to having all necessary cybersecurity protocols in place and complying with the relevant data protection laws and regulations, as well as implementing ongoing staff training and knowledge updates.

Should the worst happen and a breach occur, companies must have a robust incident response and risk management strategy in place, as well as a disaster recovery and business interruption plan to ensure they get back on their feet with minimal disruption to services.

Organisations also need to understand and learn from previous cyber attacks, and shore up their vulnerable areas by carrying out internal penetration tests.

> **Over the past few years, there has been an increase in next-generation supply chain attacks**

One company that has considered these issues at length is E.ON. The European utility provider, which serves 53 million customers across 30 countries, recognised the need to expand its processes and procedures to protect itself and its customers from potential data loss via its third-party online ecosystem.

"To tackle the issue, E.ON first had to understand the risks it was exposed to," says Ran Nahmias, co-founder and chief business officer at Cyberpion, whose ecosystem security platform E.ON used to gain full visibility of its vulnerability to cyber attacks.

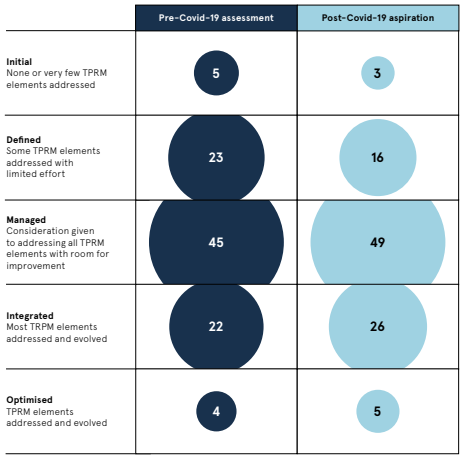
By carrying out an inventory of E.ON's internet-facing assets and the third-party assets it relies on, as well as the chains of vendor relationships, the company was able to understand its total risk exposure and allocate resources accordingly, reducing its exposure to operational disruptions and data loss.

While the complex threat from supply chain attacks remains, businesses that focus on analysing their exposure profile and mitigating the risks they discover give themselves the best chance of staying one step ahead of the hackers. ●

ORGANISATIONS ARE REALISING THE VALUE OF TAKING THIRD-PARTY RISK MANAGEMENT MORE SERIOUSLY

Deloitte, 2021

Percentage of organisations citing the following as their level of third-party risk management (TPRM) maturity



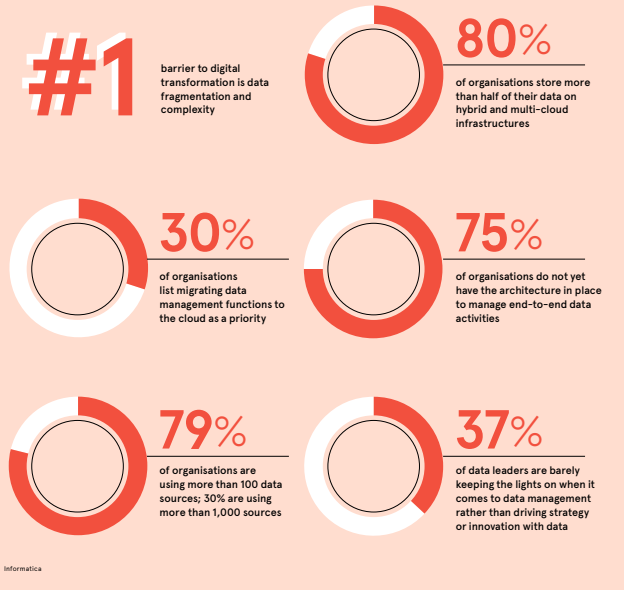
Commercial feature

Has your company reached 'data maturity'?

Data is crucial to decision-making, even more so when facing an unexpected challenge. Companies need to make sure they are serving the right data, to the right people, at the right time

IDC GLOBAL SURVEY OF THE OFFICE OF THE CHIEF DATA OFFICER

The study highlighted how critical data management is to digital transformation, noting that organisations with a high level of data maturity generate 250% more value from their data



Informatica

Data is the foundation of any strong business. If you don't have insight into how your business is operating then you won't be able to manage – let alone see – the risks you're taking. Recent history has taught us the value of planning for the unexpected. Yet beyond global pandemics, there are new technical, legal and business challenges springing up all the time. As this happens, the companies that succeed are those which can best exploit the data they have to gain insights and make decisions about where to go next.

The issue often isn't a lack of data but that companies can end up with too much data spread across different systems that require different skills to access and analyse. Nearly four in five organisations make use of data from more than 100 different sources, with 30% making use of over 1,000, while nearly 80% store more than half of that data across multiple cloud services. The data usually exists, somewhere, but all too often cannot be accessed or analysed to give useful insights.

Organisations need more than just data, they need 'data maturity', which means serving the right data, to the right people, at the right time. The data needs to be high quality, highly relevant and compliant with regulations. The correct people need access to it – whether that's the CEO who needs high-level strategic insights or a marketing manager who wants to understand the performance of a specific campaign. And the time needs to be right: it's not good enough to understand what's already happened, you need to be able to see what's happening now and have a view of the future through tools such as predictive analytics.

Yet with the business landscape constantly changing, even the data a company is managing can present risks as the important information they need to collect evolves. For instance, the amount of data relating to environmental, social and governance (ESG) issues that a business needs to understand is increasing. In the next few months, new regulations for firms operating in the UK will require reporting on the risks and opportunities presented by climate change, while those operating in the EU will need to abide by new rules requiring disclosure of the impact the firm has on climate change mitigation and adaptation.

Beyond regulation, firms are dealing with consumers who have a growing environmental, political, and social conscience about what they buy, how they buy and who they buy from. It's not enough to label a product as sustainable, businesses need to truly understand their entire supply chain to ensure every part of it actually lives up to the environmental and societal impacts they want to claim on the final product. Conversely, suppliers need to ensure they can deliver high-quality data about what they're supplying; companies themselves will increasingly make purchasing decisions based on the accountability of the supply chain they're hooking into.

One answer is to use a standardised data management platform that can deliver this level of maturity by ensuring the right level of data quality, compliance and access is available to help staff drive business decisions. This process doesn't necessarily require thousands of hours of manual work; increasingly machine learning and AI can be leveraged to ensure that the data is of high quality and that its presentation complies with GDPR and other governance rules, for example masking personal data where necessary.

With this in place, firms can better understand the data they've gathered and turn it into actionable insight. As Greg Hanson of Informatica puts it: "Our intelligent data management cloud has helped organisations drive acquisition and retention with a more accurate view of a customer and their interactions with the business."

He points to the example of Verizon, who gained better insight into their customers journeys through having a cohesive data management platform. As a result they were able to deliver self-service digital resources that ultimately reduced call service volumes by 26 million a year.

> **Truly mature organisations will rethink data management implementations and make the strategic decisions that will allow them to identify risks, pivot quickly and drive value**

The pandemic saw organisations of all kinds pivoting to a digital-first approach and dealing with fast-changing levels of demand. Those that were able to implement, or were already implementing, intelligent data management experienced huge benefits. NYC Health + Hospitals, the operator of New York's public health system, was able to make use of intelligent data management to streamline its response. This covered everything from ensuring healthcare workers had better diagnostic tools to the rapid creation of dashboards to document and forecast the impacts on the service. The technology now in place can be reapplied to any future, large-scale health events.

In a different field, meal delivery firm HelloFresh was able to rapidly scale as it experienced increased demand as people opted to eat at home. This is because its robust analytics and forecasting systems meant that change in demand was immediately obvious to those who needed to see it, even with most employees working remotely. By definition, it is not possible to plan for unpredictable events, but when they happen, ensuring that high-quality data is immediately accessible to the right decision-makers means they can respond quickly and appropriately.

The pandemic and ESG regulations are just two examples of how the risks faced by businesses will continue to shift – both through sudden shocks and as legislation, technology and the consumer environment change. Businesses need to evolve to match changing risks. Those that succeed will be the companies that use data on past performance alongside real-time updates and predictive forecasting to make high-quality choices about how they operate.

Too often, data management as a discipline hasn't received the priority or focus it deserves, but if it's done intelligently it can actually push a business forward. Understanding the risks means understanding the opportunities. As Hanson puts it: "Digital maturity is a continuous process, not an endpoint. Truly mature organisations will rethink data management implementations and make the strategic decisions that will allow them to identify risks, pivot quickly and drive value."

For more information please visit informatica.com/platform

Informatica