MARSH JLT SPECIALTY

INSIGHTS | NOVEMBER 2019

# Digital Supply Chains Require Collective Approach to Cyber Risk

As supply chains undergo rapid digital transformation, the increased interconnectivity and reliance on common technology and platforms means that cyber risk needs to be seen as a collective responsibility.

Technology is dramatically transforming the business models of individual companies and entire industry ecosystems: from the outsourcing and offshoring of basic IT and data processing services and manufacturing of the late 1990s and 2000s, to hyper-scale cloud transformation and the fully automated manufacturing, logistics, and inventory management systems that underpin modern trade and distribution of goods and services. As organizations and their supply chains rely increasingly on technology and a larger array of third-party providers, they face increasing challenges to keep up with, understand, and control the risk.

Scratch below the surface and you'll find that digital supply chains are highly complex and, often, opaque. Each layer is tightly integrated and connected, and it can be difficult to see the boundaries between organizations and suppliers, and the responsibilities and controls that each has in place. A relatively small group of technology companies provide organizations and governments around the world with IT and communications infrastructure, software, data processing, and network-related services. The top three cloud providers, for example, account for over half the entire market. At the same time, physical supply chains are becoming increasingly reliant on platforms and technology to exchange data, manage manufacturing and distribution, and transact with third parties.

Digitization brings major benefits, but also increased and new cyber risk to all parties. The lack of full transparency along the supply chain makes it difficult for organizations to properly assess cyber risk and to gain assurance about the security and integrity of third parties. A supply chain is only as strong as its weakest link – a vulnerability at one vendor or supplier can compromise the entire digital supply chain. This was dramatically demonstrated during the WannaCry ransom attack in 2017, when vulnerabilities in a single software platform disrupted over 200,000 computers in 150 countries, causing over $10 billion in losses.

## Disconnect in Views of Supply Chain Risk

The Marsh Microsoft 2019 Global Cyber Risk Perception Survey revealed an interesting disparity in how companies view the risks they and their partners present to the supply chain. Only 16% of respondents said they pose a risk to their supply chain, but 39% said the cyber risk posed to them from their suppliers was

MARSH

somewhat high or high. For large companies, the disconnect was even greater – 61% of large companies viewed the cyber risk posed by third parties as somewhat high or high, but only 19% perceived themselves as a risk to their supply chains.

The survey also revealed a disparity between the cybersecurity measures and standards that organizations apply to themselves and those that they expect from suppliers. Generally, respondents were more likely to set a higher bar for their own organization's cyber risk management measures than they set for their suppliers, for example, 56% of organizations said they expect suppliers to implement awareness training for their employees, yet 71% said that they had implemented such a requirement for themselves. Such disparities could lead companies to think their suppliers are less prepared to manage cyber risk than they themselves are, thus eroding trust in the supply chain.

The disconnect in perceptions of risk posed to and by supply chain partners likely reflects a low level of confidence in the ability to prevent or mitigate cyber risks posed by commercial partners. Just under half (43%) of those surveyed said they were not confident in their ability to prevent cyber threats from at least one of their third-party partners. The lack of confidence was highest when looking at freelancers and consultants (30%) in the supply chain. Almost a quarter (23%) were not confident in their ability to manage cyber risk from suppliers of outsourced business processes.

## Socio-political Risk

With growing reliance on IT systems and data, supply chain resilience is emerging as a wider societal and political issue. Digital systems are now essential for the provision of critical services, from energy to healthcare, yet the infrastructure and services that underpin them are often global and interconnected, and therefore exposed to geopolitical risk and subject to regulation.

As reliance on digital supply chains has increased, cybersecurity and continuity of service has come under scrutiny, particularly in key industries such as banking, utilities, and pharmaceuticals. For example, the UK financial services regulator has prioritized operational resilience for banks following a sharp rise in service outages, which were largely the result of hardware or software glitches.

Increased reliance on technology and lack of transparency on cyber resilience could well drive future regulation, especially for critical services. However, the Marsh Microsoft survey found little appetite for government intervention on cybersecurity – only 28% of businesses regard government regulations or laws as an effective way of improving cybersecurity, while only 37% regard soft industry standards, such as NIST and ISO, as being effective in doing so.

## Collective Responsibility

The Marsh Microsoft survey suggests companies have further to go when addressing cyber risk in their supply chains. It found that only one-third of respondents had carried out a supply chain or vendor risk assessment in the previous 12 to 18 months, and that just 18% said that they plan to do so. Less than a quarter of companies had quantified the cost of replacing sensitive data lost by a third party.

In an interconnected world, every organization needs to understand how cyber risks affect supply chains, and must also play a role in building shared security. Building resilience is challenging, but companies increasingly recognize they have responsibilities to facilitate cyber resilience in the supply chain. Forward-thinking players in some industries are now driving minimum standards and providing advice and support to customers and suppliers throughout the value chain.

Despite increased investment in and prioritisation of cybersecurity, business confidence in the ability to manage cyber risk has declined. Some 79% of respondents to the Marsh Microsoft survey ranked cyber risk as a top five concern for their organization, up from 62% in 2017. Yet those saying they had 'no confidence' in understanding and assessing cyber risks increased from 9% to 18% and from 12% to 19% for preventing cyber threats.

As the reliance on technology and digital supply chains increases, a cybersecurity strategy that focuses purely on protecting the organization – "barricading the castle" – will not suffice. There needs to be a shift from focusing solely on enterprise security to embracing responsibility for network security across the supply chain. Managing supply chain risk is a collective issue, recognizing the need for trust and shared security standards across the network, including the organization's cyber impact on its partners.

For more information on Marsh's solutions to help you understand, measure, and manage supply chain risk, send an email to cyber.risk@marsh.com or contact:

JANO BERMUDES
Head of Cyber Risk Consulting, UK and Ireland
jano.bermudes@marsh.com