KPMG

# Digital Supply Chain - the hype and the risks

While every business wants to harness the speed to market that new supply chain technology can offer, they are also opening themselves up to malicious cyber-attack if they don’t take the right precautions.

February 2018

KPMG.com.au

Customers of today are connected, informed and empowered, and continually demand more choice of products, greater flexibility in delivery options and faster service from the businesses that they deal with. These expectations, combined with rapidly changing business models and channels to market, are putting previously unseen pressure on supply chains to be agile, flexible and adaptable to customer demand signals.

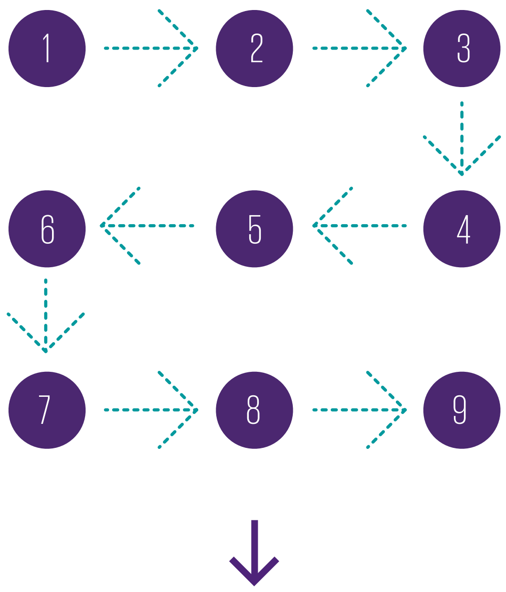
As a result, organisations are making significant supply chain technology investments, with a recent study by Gartner valuing the supply chain technology market at $13 billion in 2017, up by 11 percent on 2016, and on track to exceed $19 billion by 2021[1].

Technology investments are driving the supply chain evolution from linear, responsive-driven flows to interconnected and predictive smart networks enabling organisations to create 'Connected Customer Enterprises'. This puts the customer at the core of how products and services are designed and delivered, to meet unique customer value propositions.

Industry 4.0, the Internet of Things (IoT) and a plethora of new technologies are enabling supply chain partners to sense, predict and respond more efficiently to consumer demand signals. Those that embrace these technologies are experiencing significant uplift in supply chain performance including:

- enhanced service levels
- reduction in inventories
- improved transport flows and costs
- reduced volume of returns
- significantly improved overall customer experience.

**Technology investments are driving the supply chain evolution from linear, responsive-driven flows...**



**...to interconnected and predictive smart networks enabling organisations to create 'Connected Customer Enterprises'.**

[1] Source: Garner Newsroom, Gartner Says Supply Chain Management Market Will Exceed $13 Billion in 2017, Up 11 Percent from 2016, Stamford Conn June 2017

# Some of the most hyped supply chain technology enabled improvements include:

### Robotics:

- Chat bots are taking online customer service to the next level, enabling personalised and customised order, returns and claim management.
- Optimising warehouse flows and processes. For example many leading organisations such as Amazon run fully automated warehouse and dark stores reducing labour and energy, and improving asset utilisation.

### Auto replenishment to home:

- Consumers no longer need to keep a shopping list and trudge through the supermarket for pantry staples as auto replenishment to home has been enabled through technology such as Dash Buttons and Amazon Alexa.
- Microsoft is working with Samsung to design a smart fridge for a leading Australian retailer which will enable full automation of the fulfilment of fridge items for consumers.

### Facial recognition technology:

- KFC is trialling facial recognition technology to design a meal for consumers based on previous orders and the consumers' perceived mood.

### Driverless vehicles, drones and on-board technology:

- GPS and track and trace devices are optimising transport routes to reduce congestion and enabling major efficiencies for the economics of last-mile delivery.
- Domino's Pizza completed the first commercial delivery of food by a drone in 2016.

### Smart labels, QR codes and blockchain technology:

- Enable consumers to scan products and harness specific information to better understand product provenance and supply chain performance. For example, cold chain compliance or ethical and environmental factors.

By 2020 there will be 30 billion connected devices as part of the global IoT base, up from 14.5 billion in 2015[2].

Paradoxically, the reasons that make these technologies so valuable to companies also makes them vulnerable. The nature of having the devices interconnected and allowing external parties such as customers 'inside the walls' of your secure organisation means that you are opening the number and type of 'attack vectors' into your company's systems.

All of these emerging supply chain technologies are enabled via a myriad of access points, sensors and scanners. These devices are often physically dispersed and are not top of mind for organisations' IT security design, which exposes organisations to significant supply chain security risks. Some estimate up to 80 percent of security breaches occur through the supply chain[3].

[2] The Internet of Things is here and growing exponentially, October 2017 (press release), HIS Markit, Colleen Seery

[3] Combating Cyber Risk in the Supply Chain, SANS, 2015

# Case studies

Cyber criminals and hackers are always looking for the easiest route into an organisation's systems and data. They are realising that the shortest way is not through the front door, but through the 'weaker links' that make up a digitally enabled supply chain.

"Since 2014, more than 114,000 suspected cybercrimes have been reported in Australia - 23,700 during the past 6 months alone."

**Prime Minister Malcolm Turnbull, June 2017[4]**

This means organisations are not only faced with the challenge of implementing new supply chain technologies, but also with adequately securing them.

There are a number of examples where vulnerabilities in the supply chain have been identified and actively exploited. Attacks take many forms from Trojan attacks to Distributed Denial of Service (DDoS) events.

1. Hacktivist groups took down large portions of the internet through multiple coordinated DDoS attacks. Global DNS (Domain Name System) provider DynDNS responsible for aligning domain names to IP addresses was inundated with DNS lookup requests from hacked IoT devices (i.e. webcams and printers). Major services such as AirBNB, Amazon, GitHub, Netflix, Paypal and Twitter all experienced multiple outages as a result of the event. (2016)
2. An Australian Government department was subject to national media attention when a third party managing the maintenance of speed cameras inadvertently used a USB infected with the 'WannaCry' virus to make updates across a number of devices. As a result of the infection the Government was forced to review the legitimacy of all fines delivered during the period of infection. (2016)
3. Notpetya exploded across the world taking out businesses from shipping ports, supermarkets, hospital services, advertising agencies and law firms – even causing the Cadburys chocolate factory in Hobart to grind to a halt. (2017)
4. A recent security flaw has been discovered that can be used to hack into any Wi-Fi device. The Key Re-installation Attack (known as KRACK) exploit involves replacing the Keys used to authenticate to any Wi-Fi device. This can be performed from anywhere within the Wi-Fi's range and can be used to steal any data transmitted to or from the device. The solution is to update the firmware on each of the devices, which may take some businesses months or even years to complete. (2017)

Importantly as of Feb 2018 there will be increased legislative requirements for organisations to report data breaches. The Privacy Amendment (Notifiable Data Breaches) Act 2017 established a Notifiable Data Breaches (NDB) scheme in Australia. From 22 February 2018, data breach notification will become mandatory for all entities required to comply with the Australian Privacy Act.

By some estimates 44% of Australian businesses are not fully prepared for these changes[5].

[4] Cyber Attacks Rife in Australia, AFR, July 2017, Patrick Durkin

[5] Businesses unprepared for new data breach notification laws, 29 Jan 2018, Yolanda Redrup, AFR

With new applications for digital supply chain technologies emerging daily, we are at the beginning of the digital supply chain journey. As these smart and interconnected networks increase in sophistication and complexity, so too will the potential risks and impact of cyber-attacks. Organisations that understand and manage the breadth of their interconnected supply chains and their points of vulnerability and weaknesses are better placed to prevent and manage issues.

As cyber crimes are becoming increasingly prevalent and sophisticated we encourage organisations to consider cyber risk from a holistic perspective.

### Moving targets require big guns:

Cyber security is a business issue and the conversation has made its way to the boardroom. That is because the stakes are now so high and because the best measures in the world will not automatically guard against the increasing sophistication of cyber criminals. Four out of five (80 percent) of Australian CEOs rate Cyber Security as a top investment priority and amongst the top five risk areas for their business. Less than half (45 percent) believe they are fully prepared for a cyber-threat[6].

### Less obvious threats

There is no such thing as 100 percent guaranteed protection. Organisations need to understand - what the most sensitive data is they are trying to protect, and what strategies and objectives may need reviewing. The key is to prioritise. Decision support methodologies and tools can help quantify and rank cyber risk.

### Choosing your battles

It is critical to understand the Threat Actor. Organisations need to understand what the Threat Actor would be after, how they would attack, what controls are in place and what gaps need to be addressed. It is ok to have acceptable risk.

### First response plans

Prepare, Prevent, Detect and Respond. Organisations need to focus on being able to prepare, prevent, detect and respond. In the event of an attack well defined and tested response plans are required.

### Empowering employees and customers

As well as being vigilant at a network level, organisations need to embed security into their cultures and everyday practices. Cyber security needs to be a behaviour that is as instinctive as locking the office doors at the end of the day, it needs to be part of business as usual.

## Key learning:

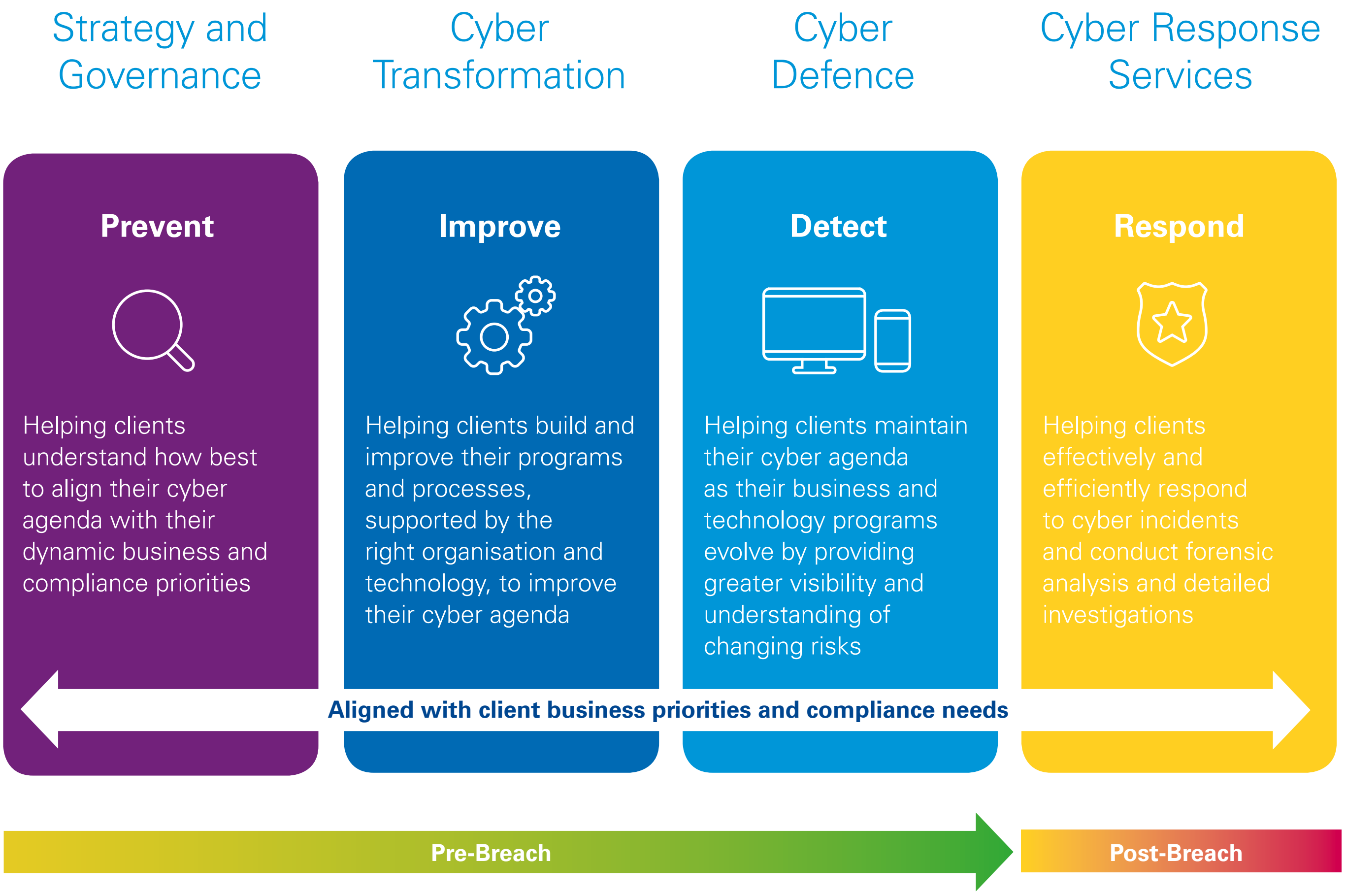
1. Effective cyber security needs a holistic approach so that investment in protecting one area isn't undermined by complacency in another. Remember, hackers and attackers will always look for points of vulnerability.
2. Board level buy in is critical. If security practices aren't driven from the top and don't permeate the entire company culture, the best measures in the world can be breached.
3. Prioritise budgets. Understand what is critical and have assurance in controls 'Protect what Matters'.
4. Collaboration is key. Be prepared to exchange concerns, experiences and learning with industry peers so everyone is in a strong position.
5. Use Experts. Security threats change and need the attention of someone who's at the forefront of the latest techniques. Targeted protection and readiness to respond are the best insurance.

While supply chain technologies bring so many benefits, organisations must diligently manage the full range of supply chain risk. Key issues include:

- Trust is regularly handed over to third party providers without proper due diligence, risk assessment or examination of controls.
- Customer expectations of companies that form part of their supply chain are rising – particularly if a company wants to provide services to government where they have to demonstrate compliance with security standards (such as ISO 2700 and NIST). If the company cannot demonstrate this level of control, or that they are at least on the journey to achieve compliance, they will not be eligible to bid for the business – and some of these contracts are multi-million dollar opportunities.
- Machinery and equipment which is reliant on old, legacy technology can be difficult to secure. This can present significant challenges and is commonly targeted by malware and viruses.

[6] 2017 Global CEO Outlook: The outlook for Australia, Disruption and growth amidst heightened uncertainty, growth, KPMG, 2017

# KPMG's Cyber Security Approach



Strategy and Governance

Cyber Transformation

Cyber Defence

Cyber Response Services

**Prevent**

Helping clients understand how best to align their cyber agenda with their dynamic business and compliance priorities

**Improve**

Helping clients build and improve their programs and processes, supported by the right organisation and technology, to improve their cyber agenda

**Detect**

Helping clients maintain their cyber agenda as their business and technology programs evolve by providing greater visibility and understanding of changing risks

**Respond**

Helping clients effectively and efficiently respond to cyber incidents and conduct forensic analysis and detailed investigations

**Aligned with client business priorities and compliance needs**

**Pre-Breach**

**Post-Breach**

KPMG has a dedicated Supply Chain Cyber Security team that brings strategic advice, subject matter expertise, flexibility and delivery of commitments. Our skilled professionals bring leading thinking in cyber response, supply chain technology and operations to identify risk areas and develop the most practical recommendations to mitigate these risks.

KPMG's Supply Chain Cyber Security Assessment and Architecture Services are focused on addressing our client's real business and technical threats. By utilising a number of different assessment techniques we identify weaknesses and vulnerabilities that are exploited by cyber threats in real cyber-attack and security breach scenarios. This is achieved by using methodologies that engage progressive tools and techniques, with a focus on non-automated, quality-driven testing.

## KPMG is recognised as a leading information security consulting services firm.

KPMG member firms have been recognised as a leading global provider in The Forrester Wave™: Information Security Consulting Services, Q3 2017. The report, aimed at informing CISOs and business leaders in selecting the right consulting partner, evaluated the network of member firms' ability to deliver information security to their clients.

### About the report

The Forrester Wave™ is copyrighted by Forrester Research, Inc. and is a graphical representation of Forrester's assessment of a market, and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments.

### Some highlights of the report include:

- "KPMG has the clearest, most direct vision… [asserting] its desire to help CISOs and boards of directors come together on information security as a business issue, not an IT issue. The company's go-to-market approach leads with vertical expertise, while it is also applying investments across global member firms in areas like data analytics to cyber security engagements."
- Client references consistently mentioned one area of differentiation for KPMG that provides high value: Jeff Pollard, Principal Analyst with Forrester writes, "Consultants with operational experience who have deeper insights on the day-to-day battles clients fight than typical service delivery personnel with just a consulting background".

# Contact Us

**Peter Liddell**
Partner – Head of Supply Chain,
Asia Pacific
+61 3 9288 5693
pliddell@kpmg.com.au

**Gordon Archibald**
Partner – Cyber Security Services
+61 2 9346 5530
garchibald@kpmg.com.au

**David Fish**
Director – Management Consulting
+61 3 9838 4141
dfish2@kpmg.com.au

**Sally Pyke**
Associate Director – Customer &
Operations
+61 3 9838 4136
sallypyke@kpmg.com.au

**KPMG.com.au**

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

Liability limited by a scheme approved under Professional Standards Legislation.

January 2018 N16151LOBS