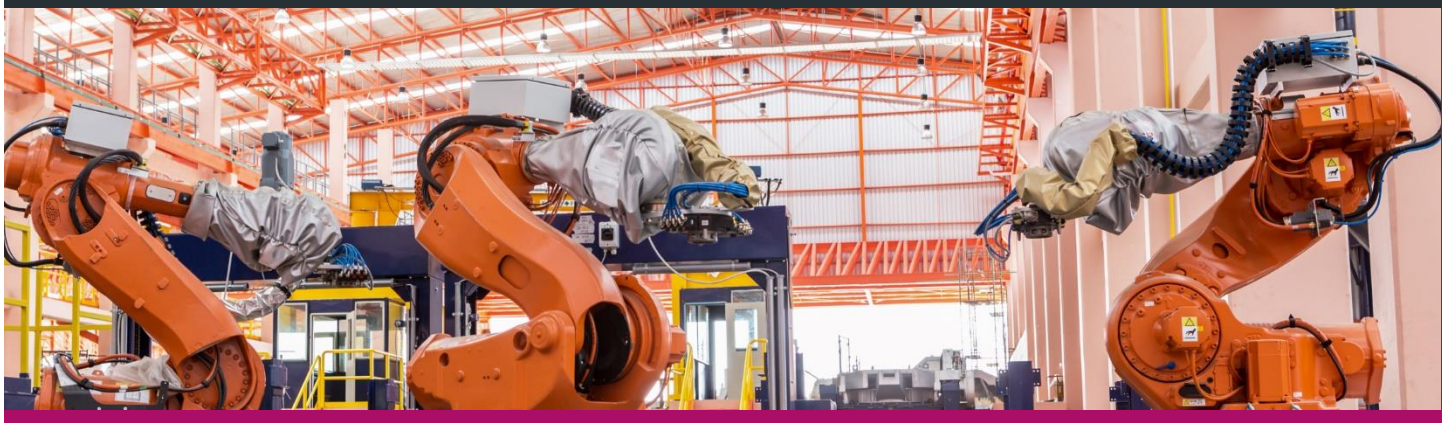

Manufacturing outlook

Spring 2023

Despite a rocky start to the year the manufacturing industry is showcasing its resilience. Results from the first half of 2023 seem to suggest manufacturers are on a slow path to recovery following the uncertain economic environment of 2022. However, there is no endgame in sight, as cost pressures at home and away remain high with little indication that this will stabilise soon. Trowers & Hamlins looks at some of the key trends and challenges facing our manufacturing sector clients and the industry more generally over the coming months.

Trends and challenges in Q2 2023

Cost and margin

Within the first three months of this year the sector showed signs of bouncing back. Output in the UK between February and March 2023 was up 0.7%[1]. Production did fall by 0.9% year-on-year in April 2023[2], but this marked the lowest decline in activity since the current period of economic turbulence started in January 2022. At the same time, costs pressures remain significant. Domestic and export input costs are continuing to rise slightly as a result of supply chain price changes and energy costs[3]. These costs are still being passed on to customers mitigating their impact, but MadeUK/BDO data suggests this is becoming increasingly harder to do as UK prices are falling and export prices stagnate.[4] This is coupled with a government retreat on some of the more favourable support measures, such as the recent replacement of super-deduction and the Energy Bill Relief Scheme.

Skills shortage

As a result of the tight labour market in the UK, the sector is continuing to face a significant skills shortage. Vacancies are on the decline, but businesses are still grappling a need to significantly bolster their workforces. In the manufacturing industry, research conducted by Make UK suggests early retirement and resignations due to ill-health are having the biggest impact on the sector and more than half of organisations are expecting 6-20% of their workforce to retire over the next decade[5]. Manufacturers are exploring options to combat this challenge such as pay increases, flexible working, and investing in upskilling and developing existing talent in the market.

Investing in digitalisation

Digital transformation is a trend to watch across sectors and manufacturing is no different with the increased use of advanced technology being used to automate manual processes. A combination of customer expectations, climate change and the skills shortage is forcing manufacturing organisations to explore how technology can be used to future proof their businesses. For example, AI monitored machines on the floor have been proven to help manufacturers quickly diagnose and resolve issues, increasing efficiency and reducing

[1] Economic Indicators, A6 Manufacturing, House of Commons Library, No. 05206
[2] Office for National Statistics: Index of Procuction, UK April 2023, https://www.ons.gov.uk/
[3] MakeUK outlook Q4 2022 https://www.makeuk.org/insights/reports/manufacturing-outlook-q4-2022
[4] MakeUK outlook 2023 https://www.makeuk.org/insights/reports/manufacturing-outlook-2023-q1
[5] MakeUK outlook 2023 https://www.makeuk.org/insights/reports/manufacturing-outlook-2023-q1

downtime. With an increasing reliance on tech comes a larger demand for valuable data to feed into AI machines and tools. Many businesses are exploring how their data is stored and protected with the cloud being a popular home for valuable data sets. However, digitalisation brings the risk of security breaches as we discuss further below.

Environmental, Social, and Governance

Environmental, Social and Governance (ESG) requirements are a primary consideration in an industry that contributes so significantly to environmental impact. There is increased discussion on how ESG principles can be seamlessly integrated into the manufacturing sector. Areas where we are seeing change includes supplier diversity, sustainable product innovation, waste management, the circular economy and a focus on employee satisfaction and engagement. The potential power of a high ESG standing is clear and pressure is not only stemming from the Government agenda but buyers, customers and increasingly funders. There is a growing emphasis on supply chains and organisations that sit further down the chain are increasingly becoming subject to external audits as larger organisations grapple with their own ESG requirements.

Trowers & Hamlins news

Trowers & Hamlins are pleased to announce that as of May 2023 we have become an associate member of the British Plastics Federation (BPF). The BPF sits at the heart of the plastics industry in the UK, and represents around 80% of the industry by turnover, covering plastics recyclers, polymer suppliers and distributors, additive suppliers, service providers, plastic processors, packaging manufacturers, equipment suppliers and more. We are delighted to be supporting the BPF as associate legal member and as Bronze Sponsor of its Award Dinner in October.

Our partnership kicked off last month with members of the BPF being invited to a bespoke seminar by Trowers & Hamlins tax specialist Nathan Williams to discuss the recent changes in capital allowances.

In wider news, Trowers & Hamlins is continuing to give specialist advice to manufacturing organisations including on investments, mergers and acquisitions and risk management. At the end of 2022, Trowers advised the shareholders of Fraser Anti-Static Techniques Limited, a Devon-headquartered multi-national anti-static equipment manufacturer, to SDI Group plc for £16.88 million. More can be read about this deal here.

IN FEATURE: Cybercrime: the silent disruptor of the manufacturing industry

In both 2021 and 2022, the manufacturing industry was the most targeted sector by cyber-attacks. The World Economic Forum recently reported that the overall five main threats are phishing attacks, ransomware, intellectual property (IP) theft, supply chain attacks and industrial Internet of Things (IoTs) attacks.

A recent IBM Report also confirmed that the manufacturing industry was most exposed to higher levels of ransomware, despite the improved detection measures adopted in 2022, resulting in business interruption, lost trade and high costs of internal investigations and disciplinary procedures.

Why are manufacturers being targeted?

Manufacturing companies are attractive to cyber criminals for several reasons including:

The complexity of the manufacturing ecosystem: manufacturers have complex supply chains and are often both consumers and suppliers. A cyber-attack can, therefore, cascade down the supply chain creating disruption to the large supply of a wider product.

Digitalisation: the incorporation of technology in manufacturing processes, while important to improve efficiencies and drive productivity, creates further routes for cyber criminals to try and infiltrate manufacturer's systems (and those of their supply chain if connected);

Data: the volume and sensitivity of data stored by manufacturing companies makes it attractive for cybercriminals to hold information for ransom; and

Strict deadlines: the additional pressure that cyber criminals can place on manufacturers to pay ransom

demands given the risk of disrupting strict manufacturing timelines that must be adhered to.

How have cyber-attacks affected the manufacturing industry?

Make UK recently reported that 50% of manufacturers have been victim of cybercrime in the last year. Cyber-attacks can lead to significant systemic impacts across a business such as downtime of operations, physical impacts and even environmental damages.

Out of those manufacturers who experienced a cyberattack, 22% suffered a cost to their business between £5,000 and £25,000 with 6% of companies losing in excess of £100,000.

The cost consequences of cyberattacks are a global issue as can be seen from cyber-attacks in recent years. For example, in February 2022, Toyota Motors suffered significant disruption after a key supplier in their supply chain was hit by a cyber-attack. Toyota had 28 production lines across 14 plants in Japan disrupted by this attack. Earlier this year in February 2023, Applied Materials, large supplier of semiconductors, announced that a breach at one of their suppliers would have a $250 million impact in the next financial quarter.

What steps should you be taking?

Despite the significant cost risks, according to Make UK, 47% of manufacturing companies in the UK do not have a formal cybersecurity protocol to follow and 66% do not have a monthly slot in their agenda to discuss cybersecurity plans.

Prevention is better than cure. It is important that those operating in the manufacturing industry have robust and comprehensive cyber protective measures embedded into their systems and implemented across their organisation.

The following key steps should be taken by manufacturing businesses of all sizes to help mitigate the substantial risks that cyberattacks cause:

1. A whole organisation approach: no risk can be managed in isolation, and cyber risk is no different. Makes sure that your internal and external IT teams are communicating with your risk teams and the board to ensure that the true risks to the business are understood and effectively managed.
2. Work with IT teams to assess internal safeguards and capabilities: managing cyber risk from the technical side does not need to be scary or expensive. Assess your current operating environment and take steps to implement solutions that are proportionate to your business risk and budget.
3. Regulatory compliance - review policies, procedures, and information governance to ensure regulatory compliance to protect against the most common cyber threats such as phishing attacks. You should also keep your software and systems fully up to date to prevent hackers exploiting any weaknesses; and
4. Formulate effective breach response plans - you should avoid taking an informal approach to incident management and should adopt a formal business continuity plan with a focus on maintaining operations in response to a serious breach and encouraging a proactive approach to cyber risk management.
5. Audit your supply chain - suppliers have access to confidential and sensitive data to facilitate the performance of their contractual obligations. You, therefore, need to audit and monitor their use, check their measures and stress test their cyber protection. To learn more please read our whitepaper on enhancing cyber resilience in supply chains: Whitepaper launch: Enhancing Cyber Resilience in Supply Chains -Trowers & Hamlins
6. Training and awareness – people are a key asset in managing your cyber risk. Create engaging culture amongst staff around cyber security so you can practice good cyber hygiene.

Get in touch

We have a specialist cyber team who are on hand to discuss any of your cyber risk management and strategy needs. Please contact one of us below for further information.

Proud partners:

BPF British Plastics Federation

PROUD MEMBER OF CBM CONFEDERATION OF BRITISH METALFORMING

Key contacts

Jamie De Souza
Partner, Dispute Resolution and Litigation
+44 (0)121 214 8847
JDeSouza@trowers.com

Moad Giebaly
Partner, Corporate and Commercial
+44 (0)121 214 8852
MGiebaly@trowers.com

Fiona Thomson
Partner, Real Estate
+44 (0)121 214 8883
FThomson@trowers.com

Rebecca McGuirk
Partner, Employment and Pensions
+44 (0)121 214 8821
RMcGuirk@trowers.com

Nathan Williams
Partner, Tax and Private Wealth
+44 (0)20 7423 8383
ndwilliams@trowers.com

Amanda Stubbs
Partner, Planning and Environmental
+44 (0)161 838 2075
AStubbs@trowers.com

Christopher Paul
Partner, Projects and Construction
+44 (0)20 7423 8349
CPaul@trowers.com

Elizabeth Mulley
Managing Associate, Dispute Resolution and Litigation
+44 (0)121 214 8864
EMulley@trowers.com

Tayler-Mae Porter
Trainee Solicitor, Corporate and Commercial
+44 (0)121 203 5675
TPorter@trowers.com