News article

Jul 2024

Manufacturing: Future Landscape of Technology

In a study conducted by Waterstons Australia, 80% of manufacturing businesses have a heavy reliance on manual work and are still using spreadsheets whilst 40% of businesses see process inefficiencies and a lack of proactivity to change as real issues.

The future landscape of technology within manufacturing not only includes the implementation of new technologies but the adaptation of current tech, people and processes to future-proof these businesses.

Looking to the past to prepare for the future, retrofitting current equipment and tech is currently a viable option for many manufacturing businesses to improve their current situation.

Charlie Hales, Managing Director, Waterstons Australia.

Through the Waterstons Innovation Fund, manufacturers are testing out new processes and software with old technology. Retrofitting existing equipment with cameras and sensors combined with machine learning. The purpose is to automatically detect quality issues in outputs as well as to proactively detect when a piece of equipment isn't operating as normal. This type of retrofitting is typically low cost, not requiring new machinery or systems.

The Human Asset

Looking at the human element of the future landscape, it's imperative that manufacturing business remain highly educated and connected with their tech. Integrating training on something as simple as Microsoft Excel and a retraining program on current technology within the business can often be a huge edge for the business.

Looking at cyber security, many infiltrations of a company's systems begin with a stolen password. The importance of your human element is imperative to the future of any manufacturing business.

Cultivating a strong company culture can sometimes be overlooked by organisations. However, ensuring your human assets and culture are cohesive, collaborated with and trained correctly reduces the risk of potential disdain from employees who could potentially leak data.

There are a multitude of instances like this which can incur serious consequences to a business. So, creating a cohesive culture is imperative in protecting your business.

Sustainability is Key

With the increase in consumer demand for sustainably produced products, the future of manufacturing will be dominated by those using sustainable practices. By better defining what your current emissions are, manufacturers can work on strategies to reduce them.

This will help with tenders, provide better supply chain visibility and identify opportunities to reduce costs. Becoming more sustainable through technology not only creates a better environment but puts the business into a more favourable position with consumers and potential tenders. It also ensures a better working environment for employees.

Incorporating technology into this element, organisations should look to improving software's, processes and technology for a seamless transition into more sustainable business practices.

The Long View

Long term future gazing is improved supply chain visibility and collaboration through better integration between manufacturers and their suppliers. The ideal landscape is one whereby manufacturers can share live views of forecasted demand with their suppliers to promote improved communication and preparation.

This can work both ways where suppliers can share their available capacity. For many businesses, this would represent a complete change of culture and involve strong processes, technology and data around forecasting, MRP (material requirements planning) and production capacity.

We're already seeing a huge amount of robotics within manufacturing. However, Waterstons predicts that robotic process automation (RPA) to automate repetitive tasks within systems, such as order management, order fulfilment and customer enquiry management, will continue to make the lives of manufacturers easier.

Robotics doesn't mean the purchase of expensive and fancy robotics machines, RPA improves system processes (e.g. through integration) to optimise and automatically process tasks. However, if your organisation needs a technological 'make-over' and high-tech robotics is the right fit, the costs associated with purchasing advanced robotics equipment are much higher.

Larger global companies have already seen the value in their investment, and we will continue to see a rise in RPA in the coming years.

Cyber Security is Crucial

Your business might have anti-virus software and an internal IT team which does basic checks on your systems. This may seem like enough as maybe you're one of the lucky businesses that haven't been breached. However, simply having the above is not sufficient.

Cyber security attacks are growing each day, malicious actors are becoming more volatile, targeting new industries and to assume the manufacturing industry is immune is unwise and will not future proof your business. We need only look at recent headlines to see the disastrous effects of online adversaries.

As cyber security experts, we have innate experience in this sector. By way of an example (due to the sensitive nature of cyber security breaches, the names of these businesses in this example are protected), in 2022, Business A was breached when a malicious actor (hacker) infiltrated their system through credentials which were not protected.

The malicious actor was in the system for many weeks preparing for their attack. Once breached, supplier transaction systems were shut down and Business A lost large clients and revenue due to the breach, operations were halted for weeks. Business B, a customer of Waterstons, experienced a similar breach.

After our experts promptly responded to the breach, Business B was back up and running within 48 hours and ultimately benefitted from the lack of protection undertaken by Business A. Our customer ended up winning the revenue from Business A.

This is just one example of the difference between having crucial cyber security processes in place. From your HVAC systems to your CCTV, your machinery to your software, nothing is off-limits or too difficult to get into.

Australia is well behind Europe in terms of taking cyber security seriously. Lack of patch management, planning and incident response plans are rife throughout all industries and the longer you leave 'Cyber Security' out of your business plan, the more vulnerable your organisation becomes.

The need for incident response plans including consultation with cyber security experts and training for human assets is imperative to the longevity of the business and mitigating future risk.

Thanks for partnering with us on this article, https://australianmanufacturingnews.com/manufacturing-future-landscape-of-technology/