Waterstons
we're with you

+44 345 094 0945
www.waterstons.com

Article

May 2022

The link between manufacturing profits & data protection

Manufacturing and technology are irrefutably linked. If our technologies are not optimised, how can we expect our manufacturing processes to be? A technological breakdown of the technologies driving your manufacturing process can bring your supply chain to a grinding halt. While manufacturers strive for uptime and higher production rates, the complexity of their technology portfolios grow and in turn, so do the requirements to protect these systems and their data from such a breakdown.

In too many cases, an "It's been fine for the 'X' number of years, it's probably not an issue." mentality has been applied to Cyber Security and data protection. Which is understandable for organisations that are yet to see an active breach. Continuing this mentality has proven to be a financial pitfall for too many manufacturers.

The factory floors are humming, trucks are leaving the loading dock and aside from a basic anti-virus, e-mail spam filters and file access permissions, not much more has crossed the minds of manufacturers to that their business is secure.

However, with recent changes to Cyber Security Insurance Policy requirements in Australia, increased fines for non-disclosure of data breaches and cyber-attacks focused on destroying and encrypting data *(that most of the time, you can never get back)* and devices critical to keep those orders filled, Cyber Security is a growing blind spot that can lead to enumerable damage.

One of the first and most prolific examples of the damage these attacks can inflict on a manufacturing organisation occurred back in 1996. Omega Engineering suffered major damage to the data required to continue production of 25,000 different products and as many as 500,000 customisations to them, all of this ultimately leading to $12,000,000 in losses, their competitive footing within the market and layoffs of 80 employees.

All of this, simply because a scorned ex-IT Manager sought a personal revenge on the organisation. This individual left a 'logic bomb' (a program set to run after a certain date) which deleted this data weeks after his departure.

Granted, this breach happened many moons ago, but this damaging breach was one of many major examples of manufacturing organisations grasping the link between the safety of their digital information, their production capabilities and ultimately, their profits.

How do we identify risks now and what are the common risks we should be looking out for?

In a recent study conducted by universities in the US, it was concluded that manufacturers must first consider the potential threats to their system. This is a broad statement *for a reason* as threats and vulnerabilities within one's system can span from human threat (internal or external) to just a hot day where HVAC systems malfunction. You can read more from that report here.

Once the company evaluates their threats and vulnerabilities, the company must then assess the likelihood of each event to truly determine the protection priorities.

Considering the threats/vulnerabilities and assessing their likelihoods is a complicated process and most companies do not have the internal capability to conduct these thorough sweeps and manage the systems to protect them.

This is where the experts come in

Waterstons has worked with manufacturing companies for close to 30 years and appreciates the complexities within one's business. Working with you and not just for you.

Our cyber security experts in Australia can tailor a bespoke service for your business which spans not only a full business evaluations and analysis report of threats and vulnerabilities but the most appropriate solution for the business, whether it be externally managed security, implementing a cyber security strategy, compliance and governance protection, Essential Eight & ISO27001 and more.

Have a no obligation chat with us today.

Have a question or need advice?

Please complete the short contact form below to send a message to our team and one of our consultants will get back to you within 24 hours. Thanks.

Contact us