CBiS Supports Effort of the Aluminium Sector to Improve its Digital Resilience

Increased connectivity and computing power in ever-smaller mobile devices are paving the way not only for smarter products and services, but also for smarter manufacturing. The Metals industry and its supply chain are being transformed by developments in digital technologies, particularly by connectivity between their information systems and the innumerable components forming their operational infrastructure. New data-enabled product and process engineering lifecycles and manufacturing execution are paving the way for the sector's dive into the Industry 4.0 arena.

However, accompanying their positive effects are the challenges of implementing and adopting cutting-edge technology and its applications in the sector. With current technology developments new challenges emerge, particularly derived from the security of the data, information and knowledge driving the sector. Today, cybersecurity is expected to be among the top priorities for any manufacturing company.

The Aluminium sector is no exception. A major cyber-attack in March 2019 on a Norwegian aluminium company that employs 35,000 people in 40 countries raised awareness of the digital risks faced by every part of the Aluminium industry and its supply chain.

Dr Alexeis Garcia-Perez has collaborated with the Aluminium sector on the subject of cybersecurity since 2017. In his role as a member of their Advisory Board, Alexeis has brought the subject of digital resilience to a growing number of executives through the Future Aluminium Forum, first in Italy (2018) and then in Poland (2019). Although a presentation to the industry is planned in May 2020 in Quebec, Canada, we sought to capitalise on the growing interest on the subject of cybersecurity and Alexeis's network of senior executives within the sector. CBiS then decided to bring the industry to Coventry University in an effort to transfer relevant knowledge between the two parties and increase the impact of our research. An international workshop on cybersecurity in the Aluminium industry was then organised with funding from the University's Strategic Priority Fund.

The call attracted almost 30 C-level executives from Europe and the US to a workshop held at Coombe Abbey on the 26 and 27 February. Participants included CEOs, CTOs, CIOs and MDs from companies such as European Aluminium, ALFED, Aludium, Novelis, Costellium, AMETEK, Siemens and REEL, as well as IBM (USA and Germany) as a provider of technical cybersecurity solutions to the sector. Coventry University was represented by colleagues from the two Research Centres at the Faculty of Business and Law.

During the two-day event, participants exchanged knowledge about the dynamic cybersecurity landscape where the sector operates. Presentations from key industry players and from Coventry University colleagues helped the sector understand the multi-dimensional nature of the problem of digital resilience in Aluminium. Of particular relevance was a tabletop exercise where participants were able to collaborate in outlining the strategy to prepare, respond and recover from a cyber-attack to the sector.

The workshop helped raise awareness of the role of the management board in improving the digital resilience of the Aluminium sector, and the need to address cyber security as a strategic issue as opposed to a purely technology challenge. Through its ongoing relationship with the Aluminium sector, CBiS will continue to lead efforts to support the manufacturing sector in addressing the cybersecurity management challenges.

"The workshop on cybersecurity was very well organised and included plenty of time for discussion and networking. Cybersecurity was discussed from business, legal and academic perspectives, which gave participants a very good overview of all threats and opportunities for improvement. I particularly enjoyed the interactive crisis simulation, in which we had to respond to an escalating cybersecurity crisis in small teams. The crisis simulation highlighted that cybersecurity should be a top concern for any staff member in any organisation as the implications of a cybersecurity breach can potentially be far-reaching and impact an organisation's reputation, profitability and employee health and safety."

Kelly Roegies, Communication Manager, European Aluminium

"I found the Cyber Security Workshop very informative with an excellent mix of presentations and interactive practical workshop exercises which did a great job of communicating what a big important topic this is. I have already communicated the main takeaway message for me which was that we should be putting a Cyber Security Strategy in place and assessing our digital resilience to the possibility of an attack on our company."

Peter Unwin, Global Industry Manager (Metals), AMETEK