Cybersecurity Roundtable – Institution of Chemical Engineers (IChemE)

1. Executive Summary

- Cybersecurity is fundamentally a human challenge, requiring not only technical skills but also the right mindset and culture.
- While gaps in cybersecurity understanding exist across the population and key professional groups, there are also examples of good practice.
- Cybersecurity depends on physical security and supply chain integrity, which are often overlooked.
- Chemical and process engineers are central to the UK's Critical National Infrastructure, both in its design and operation.
- The Institution of Chemical Engineers (IChemE) has a critical role in promoting cybersecurity awareness, integrating it into professional development, and providing relevant training.

2. Introduction and background

Cybersecurity is a significant and growing concern. Our economy and society rely on a wide range of digital infrastructure, yet these critical systems are under unprecedented threat, as illustrated by recent attacks in the UK on the Synnovis laboratory and on Southern Water. The latest government research found that around half of UK businesses had experienced a cyber-attack in the previous 12 months.

Chemical engineers design, operate and optimise a wide range of critical infrastructure where cybersecurity is paramount, ranging from nuclear power plants to biochemical reactors. The continued security and safe operation of these facilities is critical both to public confidence and to wider environmental and public wellbeing. IChemE convened an expert roundtable in January 2025 to explore this topic, and this write-up presents an anonymised summary of key themes from the conversation.

3. Emerging themes

3.1 Workforce, cultural and skills challenges for cybersecurity

A dominant theme in the discussion was the central cybersecurity challenge posed by the human component of any system. A number of connected topics were discussed:

The first issue noted in this area was demographic – the existing cybersecurity workforce is ageing and facing a drop-off in numbers as existing workers retire. There were serious

concerns about what will happen when this expertise is lost, although some examples of good practice in expanding the workforce were noted, for instance a bursary run by the Security Institute being shown to help bring new and more diverse talent into the profession. There was also serious concern about visa restrictions making it harder to address shortfalls in talent in this area, and the rise of "snake oil salesmen" claiming expertise in this area without holding any relevant qualifications.

Participants expressed a concern about the lack of cybersecurity skills and knowledge among (a) c-suite level professionals, (b) people working in critical infrastructure, (c) the workforce more generally and (d) older generations in particular. Particular gaps were noted regarding understanding of good practice and common vulnerabilities faced by IT systems.

A number of other cultural issues came up in conversation including: a lack of intellectual and emotional investment in the cybersecurity plight of the country on the part of the public (with cyber attacks on the UK receiving much less attention or outrage than a physical attack would); widespread complacency about cybersecutrity threats facing the country (e.g. a lack of concern about the threat of Russian sabotage or the data risks of TikTok); and a widespread attitude in industry and beyond that ‘it couldn’t happen to us’.

Attendees felt that as much as any specific piece of cybersecurity knowledge or particular skill, the most important thing to do would be to train people with the tools and behaviours to empower them to be more sceptical and risk aware. There was a desire to see people shift from a more trusting mindset to a more sceptical one when it came to cybersecurity. It was felt that this could be promoted through a shift in educational practices to encourage this kind of thinking from a young age, and that this could be achieved through a greater emphasis on critical thinking, with people being encouraged to actively seek to disprove hypotheses instead of simply looking for evidence to support trusted theories. More positively, it was noted that process engineers had historically been extremely successful in making safety central to their professional culture and that this was a model that should be replicated when it comes to achieving a more risk-aware culture in cybersecurity.

3.2 Fundamental differences in operational technology (OT) and information technology (IT) and issues posed by their interaction

OT and IT face fundamentally different challenges and constraints, and as a result embody drastically different design approaches. OT is designed to be long-lasting, highly safe and reliable, and in operation continuously. IT systems, in contrast are built for flexibility, scalability, and frequent updates to accommodate evolving business needs and cybersecurity threats. OT systems are designed to be in place for the long term, whereas IT systems have much shorter life cycles.

It was noted in discussion that many OT systems were not originally designed with cybersecurity in mind, leaving them susceptible to cyberthreats and in some cases imposing restrictions on cybersecurity - example instance some legacy OT equipment is simply unable

to implement the most cutting-edge IT security such as cryptography. This is a key issue in the UK given the amount of legacy OT equipment still in use.

There was some discussion of the integration of OT and IT. Bringing these two more closely together was felt to hold out the potential of a range of benefits such as improved efficiency, faster decision-making, but it was also acknowledged that this integration would expose OT equipment to additional cybersecurity risks. There were some examples of companies taking very permissive attitudes to risk in this area, and attendees expressed some trepidation at some of the practice that they had encountered.

3.3 Physical security and supply chain security as critical components of cybersecurity

Attendees noted that achieving (cyber)security was not simply a matter of protecting one's IT systems in isolation, but rather required actively managing the risks of a number of connected systems. For instance, there was a discussion of the importance of actively interrogating the security of one's supply chain (for instance through reviewing annual vetting records, dip sampling or site inspections), the vulnerabilities presented by workers' domestic environments and their families, and the need to physically protect OT systems from attacks – as exemplified by Stuxnet, where malware was introduced via infected USB drives. Without carefully managing the risks of these wider systems, it was noted, even the most advanced IT system can be compromised with ease.

3.4 Good practice exists but is not embedded or widespread

Participants were optimistic that pockets of good practice do exist in cybersecurity, and in cybersecurity training. While there was a significant skills gap among the workforce and population, attendees were clear and optimistic that there was a huge opportunity to make a difference through greater provision of training. There was particular interest in upskilling engineers and there was some discussion of what it might look like, with suggestions including setting out new best practices for HAZOPs to include cybersecurity, and for institutions such as IChemE to take a lead on upskilling the workforce.

4. Conclusions and recommendations

- Human beings are central to the cybersecurity of any system. The right skills and knowledge is crucial, but so is the right kind of attitude, culture and norms. A key challenge for achieving cybersecurity is to shift people from an attitude of 'It can't happen to us' to being more sceptical and risk conscious. Gaps in cybersecurity understanding and awareness are present both across the population, and in key specific professional groups (although there is also encouraging good practice.)
    - ***Cybersecurity (and the promotion of associated critical thinking skills) needs to be integrated into the curriculum at all levels, and the Government should consider this a key part of any syllabus review activity.***

- Process engineering provides a strong historical example of how safety can be made central to a profession's culture. Professional bodies such as IChemE have an important role to play in developing, spreading and promoting best practice among their membership and industry.
    - ***The Institution of Chemical Engineers should explore the possibilities for providing training on cybersecurity, and consider the role of cybersecurity in continuing professional development.***
- The integration of operational technology (OT) and information technology (IT) presents both opportunities and risks – holding out the promise of improved efficiency and faster decision-making, but also exposing systems to additional cybersecurity risks.
    - ***IChemE and others should continue to explore this topic in collaboration with others.***
- Cybersecurity relies on physical security and a secure supply chain, yet all too often these wider components are overlooked, drastically increasing the risks of an attack.
    - ***Cybersecurity training at all levels needs to cover the role of physical and supply chain security.***
- Chemical engineers work at the heart of many of the 13 sectors designated as Critical National Infrastructure (both in design and in operation). The security of these facilities is vital, making both the cybersecurity skills of chemical engineers - and the availability of a sufficiently large chemical engineering workforce - crucial to their safe operation.
    - ***In recognition of the vital role played by chemical engineers in the operation of the UK's critical national infrastructure, chemical engineering should be designated as a subject of strategic national importance.***

About IChemE

The Institution of Chemical Engineers (IChemE) is the qualifying body and learned society for chemical, biochemical, and process engineers in the UK and worldwide, with over 31,000 members. Our mission is to champion the input of chemical engineers to create a sustainable future. We support our members in applying their expertise and experience to make an influential contribution to solving major global challenges, and are the only organisation permitted to award Chartered Chemical Engineer status and Professional Process Safety Engineer registration.

Find out more about IChemE and our strategic vision of Engineering a Sustainable World at icheme.org