The Institution of Engineering and Technology

Cyber skills and resilience in engineering

A summary of our new research revealing how engineering companies are preparing for a rise in cyber threats.

theiet.org/digital

Key points and recommendations

As engineering companies are at the heart of the digital revolution, they, like every other sector, face increased cyber threats. These can undermine competitive advantage, revenue growth and consumer trust for their businesses, and the growth and prosperity of the wider economy. In the summer of 2018, the IET commissioned BMG Research to survey 450 UK businesses to determine:

- **strategically how prepared businesses are** to meet cyber threats;
- **the extent that cyber security is built** into supply chains;
- **the current level of cyber skills** amongst engineers/technologists;
- **whether the availability of cyber skills** training matches needs;
- **the effectiveness and reach of cyber skills** information and guidance for users.

The IET has over 168,000 members in the engineering profession; these are represented through policy panels and expert groups. A core group was convened to assess the survey results.

The main findings from the research were:

1 Engineering and technology companies are yet to fully address the challenges faced from cyber security. One in five companies (20%) surveyed said they are not prepared, or don't feel that cyber security challenges are relevant, while 41% are partially prepared.

> **Recommendation:** That organisations do a proactive assessment to determine if cyber security is embedded into business strategy and whether capabilities are being adequately resourced.

2 Significant challenges exist in getting cyber security delivering through the supply chain. Just under a third (31%) of firms collaborate with suppliers/customers on digital issues; and only 38% of respondents include cyber security terms in contracts.

> **Recommendation:** That organisations review their supply chain risk for cyber security, and ensure appropriate contractual, technical and other methods are in place for mitigating the risks.

3 Accessing cyber security skills remains a challenge for the engineering sector. Only 35% of those that employ engineering staff at a professional level report that their business has all the cyber security skills it needs.

> **Recommendation:** That priority focus is given by government, academia and industry to skills, competencies and career pathways for cyber security roles – to ensure that engineering organisations have access to technical and leadership talent.

4 Training is not being delivered to enable engineers with cyber security skills and competencies. A high volume of companies (66%) haven't supplied cyber security training to engineering or technical staff in the last 12 months.

> **Recommendation:** That digital skills are incorporated as a key element within the competency framework of engineering roles.

5 73% of respondents say that their business keeps up to date with cyber developments that affect engineering and technology. But only 28% of respondents say that they have sought external guidance on cyber security matters in the last 3 years.

> **Recommendation:** That individuals and organisations engage in ecosystems to ensure they are sharing and developing knowledge around evolving threats and best practice, so as to develop and enhance cyber resilience in current and future operations.

For further information please contact us at **SEP@theiet.org** or visit **theiet.org/digital**