Progress and research in cybersecurity
Supporting a resilient and trustworthy system for the UK

EXECUTIVE SUMMARY

THE
ROYAL
SOCIETY

Digital systems have transformed, and will continue to transform, our world. From social networks to self-driving cars, digital technologies are changing the way people work, interact and do business.

The UK is particularly well-placed to realise the benefits of this emerging digital society. It has the advantages of supportive government policy, a strong research base and a history of industrial success.

The benefits have already been substantial, but they remain at risk. Cybersecurity in most organisations lags behind the state of the art. Attacks are increasing, and breaches can cause substantial harm to individuals and organisations. This erodes trust, and along with it, the potential benefits digital systems can deliver.

To read the full report, visit **royalsociety.org/cybersecurity**

Trust

Trust is essential for growing and maintaining participation in the digital society. Organisations earn trust by acting in a trustworthy manner: building systems that are reliable and secure, treating people, their privacy and their data with respect, and providing credible and comprehensible information to help people understand how secure they are.

Encryption is a key technology that underpins trustworthy computing. As digital technologies become ever more central to our lives, encryption becomes more important, and any weaknesses in its implementation become greater risks. Governments must commit to preserving the robustness of end-to-end encryption, and promoting its widespread use.

Modern digital systems face a wide range of risks and threats. Evidence-based guidance, including clear standards and sound practice, would help businesses and other organisations protect themselves in this risky environment. This guidance should be paired with a system of certification marks, to help consumers, investors and others understand and assess how secure they are and to inform their decisions.

Resilience

Resilience – the ability to function, adapt, grow, learn and transform under stress or in the face of shocks – will help organisations deliver systems that are reliable and secure. Resilient organisations can better protect their customers, provide more useful products and services, and earn people's trust.

Resilience will depend on businesses and others having access to high-quality, trustworthy advice and standards, as well as access to early information shared by others. These all depend on public sector institutions, which will need to be expert, transparent and have a clear remit and objective. The Government is taking a welcome step by bringing its cybersecurity functions together in one institution (the new National Cybersecurity Centre). It should also commission an independent review of the UK's future cybersecurity needs, to identify the institutional structures needed in the longer term.

Rapid progress is needed, and organisations will need stronger incentives to improve their cybersecurity, and to contribute to the security of others. Businesses and public sector organisations should regularly report against robust standards of cybersecurity practice, and should be encouraged to share information to help others.

Research

Research and innovation in industry and academia will continue to contribute to a more resilient and trusted digital environment. Research can illuminate how best to build, assess and improve digital systems, integrating insights from different disciplines, sectors and around the globe.

At the current rate of progress, research developments will not be fast enough to match defensive cybersecurity capabilities with those of attackers. To achieve a step change in cybersecurity, the UK should introduce a new, challenge-led research funding organisation.

Cybersecurity is a distinctively multidisciplinary, global, and cross-sectoral field. These characteristics make it important that UK research and practice draw on talented researchers from outside the UK, and across disciplines and sectors, including through peer review and collaboration.

Translation

Translation of innovative ideas and approaches from research drives the supply of reliable, proven solutions. This diverse set of tools and solutions is needed to tackle cybersecurity risks that are difficult to predict, and is best achieved by maximising the diversity and number of innovations that see the light of day as products.

Government should help innovative approaches get out of academia and to the market-place through its procurement activities, and by supporting ideas with large potential spillover benefits that might not otherwise be funded.

University technology transfer offices should focus on the volume of commercialisation opportunities, aiming to make it easy and attractive for researchers to commercialise their ideas. This would deliver greater long term benefits for society, rather than short term financial returns for universities.

Policy, practice and research will all need to adapt so that we can enjoy the benefits of digital systems without compromising on safety or security. The recommendations made in this report seek to set up a trustworthy, self-improving and resilient digital environment that can thrive in the face of unanticipated threats, and earn the trust people place in it.

Organisations earn trust by acting in a trustworthy manner: building systems that are reliable and secure, treating people, their privacy and their data with respect, and providing credible and comprehensible information to help people understand how secure they are.

The Royal Society is a self-governing Fellowship of many of the world's most distinguished scientists drawn from all areas of science, engineering, and medicine. The Society's fundamental purpose, as it has been since its foundation in 1660, is to recognise, promote, and support excellence in science and to encourage the development and use of science for the benefit of humanity.

The Society's strategic priorities emphasise its commitment to the highest quality science, to curiosity-driven research, and to the development and use of science for the benefit of society. These priorities are:

- Promoting science and its benefits
- Recognising excellence in science
- Supporting outstanding science
- Providing scientific advice for policy
- Fostering international and global cooperation
- Education and public engagement

Cover image
© mustafahacalaki.