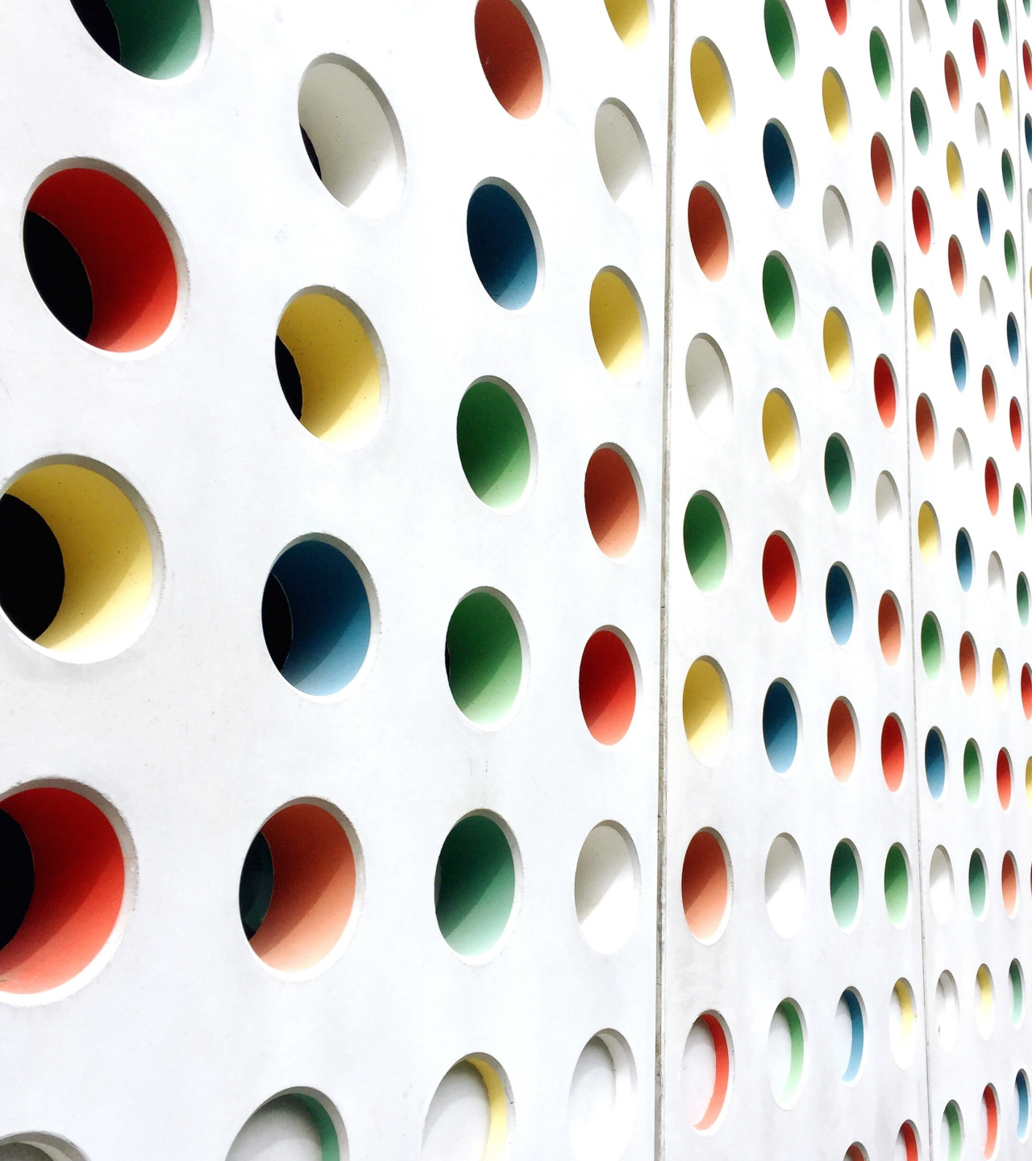

Resilience and Good Practice

DATA SECURITY

Cyber Resilience

Cyber resilience refers to an organisation's ability to continue functioning despite a cyber-attack or data breach.

New threats are appearing on an almost daily basis and, regardless of the size of the organisation, it is impossible to defend against every threat that is out there.

It is a matter of when an attack happens, not if. Cyber resilience acknowledges this, and focuses on how quickly an organisation can spot an attack and respond accordingly.

Cyber resilience combines cyber security and business security. Its aim is to prevent cyber-attacks and, in the long term, ensures the survival of the business after an attack has succeeded.

The business needs to have a robust business continuity plan in place so that it can resume normal operations as soon as possible after any attack has taken place.

International Standards – links to more info

CLICK HERE FOR ISO 27001

DEALS WITH THE IMPLEMENTATION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) TO HELP PREVENT A CYBER-ATTACK.

WEB: HTTPS://WWW.ISO.ORG/ISOIEC-27001-INFORMATION-SECURITY.HTML

CLICK HERE FOR ISO 27031

GIVES BEST-PRACTICE GUIDELINES FOR INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) TO ENSURE BUSINESS CONTINUITY.

WEB: HTTPS://WWW.ISO.ORG/STANDARD/44374.HTML

National Cyber Security Centre

The National Cyber Security Centre has created a resource that is used by businesses across the UK to outline the important steps small businesses should follow to ensure they are cyber resilient. This can be found here.

Five Steps suggested for small businesses

1. Backing up your data.
2. Protecting your organisation from malware.
3. Keeping your smartphones (and tablets) safe.
4. Using passwords to protect your data.
5. Avoiding phishing attacks

To-Do

Proceed onto the next part for
Risk Management and Cyber Hygiene