## OPPORTUNITY #8

IS THERE A WAY TO PROTECT OUR MOST PERSONAL DATA?

# PUTTING THE 'SAFE' IN DATA SAFETY

Individuals' personal data is stored in a digital safe, protecting their privacy in an environment where real-time data capture and analysis is ubiquitous

### WHY IT MATTERS TODAY

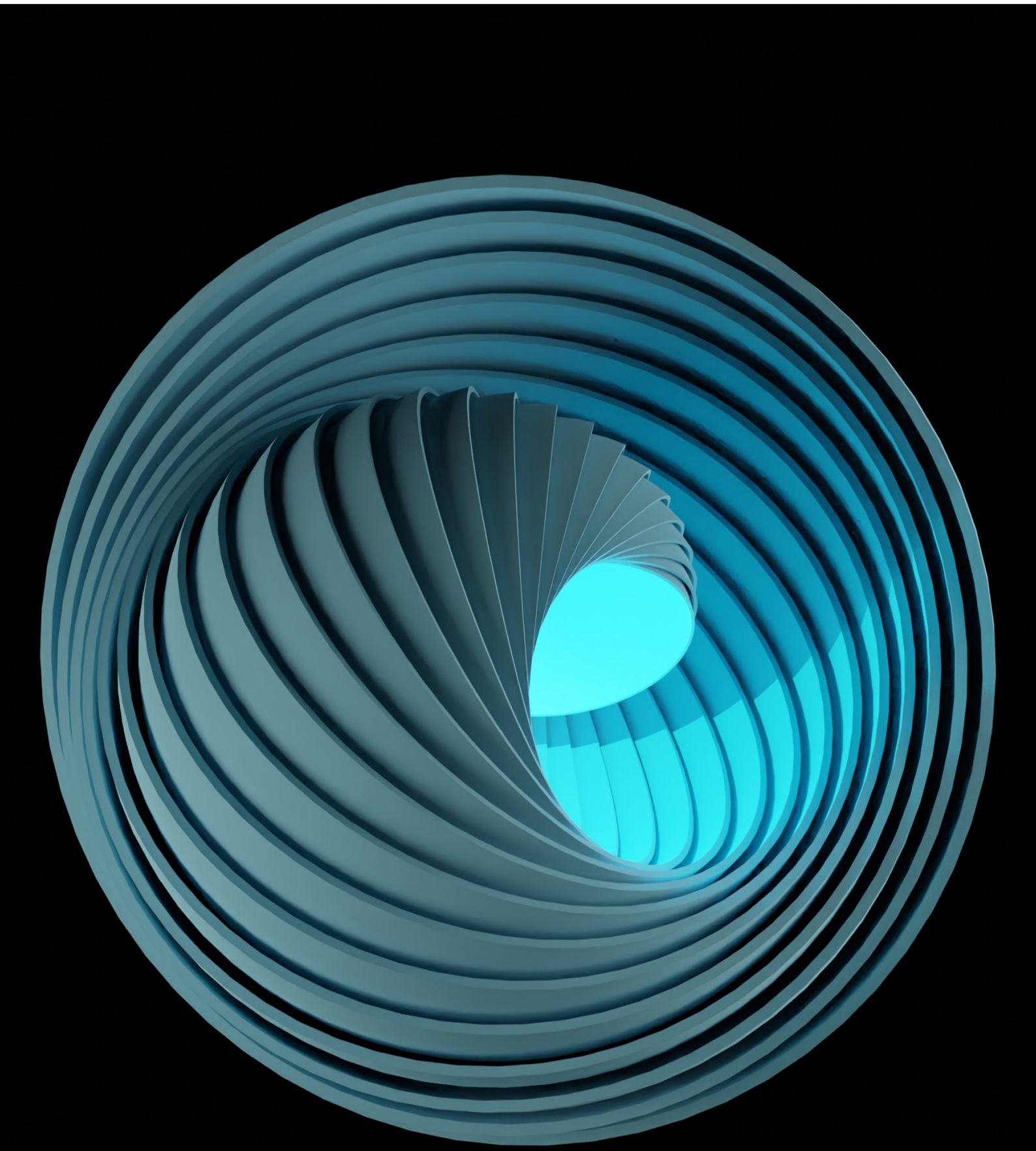
Data breaches, deletion or manipulation of critical data, disruption of services, fraudulent transactions and theft[66] led to more than 37 billion[67] records being compromised in 2020.

Overall, the direct costs of data breaches in 2020–2021 rose from $3.86 million to $4.24 million, approximately 10% year on year.[68] Valuable to cybercriminals, between 2020 and 2021, healthcare data breach costs increased from an average total cost of $7.13 million in 2020 to $9.23 million in 2021, a 29.5% increase.[69] Also in 2021, data breach costs in the public sector witnessed a 78.7% increase in average total cost from $1.08 million to $1.93 million.[70] Ransomware events cost an average of $4.62 million per attack in 2021.[71]

These include the costs of recovering a lost or stolen record and containing the associated impact but do not include the hidden costs from increased insurance premiums, operational disruptions, devaluation of trade names and loss of intellectual property.[72] The most common type of record lost is customer personal identifiable information (PII) at $180 per lost or stolen record in 2020 compared to an average of $161 per record in 2021.[73] With increasing demand for protection from such events, the global cybersecurity market is predicted to grow from around $167 billion in 2019[74] to $345 billion by 2026[75] and individuals are increasingly concerned about their personal data.

**SECTORS**

**HEALTH & HEALTHCARE · INFORMATION & COMMUNICATION TECHNOLOGY · INSURANCE & REINSURANCE · PROFESSIONAL SERVICES**



Cost per lost or stolen record

## $161 average (2021)

The most common type of record lost is customer personal identifiable information (PII)

### THE OPPORTUNITY TOMORROW

With advancing machine intelligence and the growth of quantum computing, data could proliferate at a rate that challenges cybersecurity systems to keep track of it and to distinguish between personal and public information. However, advances in storage technology, distributed ledger technology, encryption and user authentication methods can lead to new kinds of cybersecurity systems that store sensitive data in safe spaces.

'Digital safes', or digital trusts, that use novel encryption systems can enable people to perform online transactions and interact using emerging technologies such as augmented reality, feeling secure in their protection against cyberattacks. Moreover, by adopting new technologies including encryption and distributed ledger technology, a data trust can provide transparency in data sharing and auditing that shows who is using the data at any time and for what purpose, thus removing the legal and technological friction that currently exists in data sharing.[76]

### BENEFITS

As people gain confidence in the safety of their personal data, levels of trust can increase among individuals, government and business, improving societal cohesion and entrepreneurialism. Data trusts can also encourage data interoperability as well as the ethical governance of data, for example by ensuring that individuals have consented to the various uses of their data (as required by regulation in several jurisdictions around the world), removing data bias and de-identifying personal data.

### RISKS

Risks include states betraying their citizens' trust and increased vulnerability of societal well-being to unintentional or malicious data breaches.