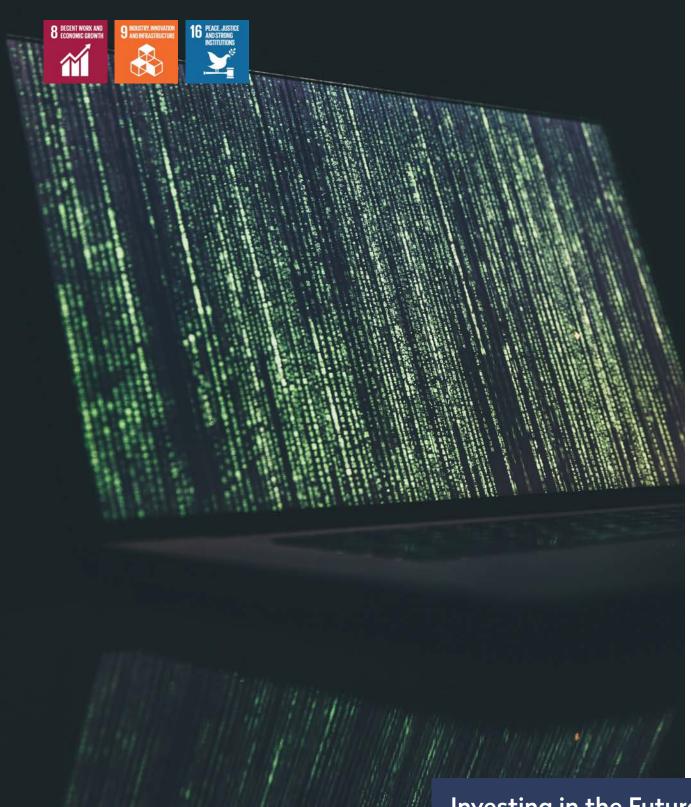
The Value of Cybersecurity



Investing in the Future

Business solutions to the Global Goals



The Challenge

Cybersecurity has become one of the most **significant ESG risks** globally.

Covid-19, lockdown and the shift to hybrid working have accelerated the digital transition in advanced economies.

Technology is now critical to global infrastructure – but this leaves us incresasingly vulnerable to cybercrime.

- More than 80% of UK organisations experienced a successful cyber attack in 2021/2022¹.
- > The average cost of a data breach in 2021 was more than £4m².
- > 2017's WannaCry ransomware attack impacted critical health services, and cost the NHS £92m.

For individuals, this represents a huge risk of fraud, identity theft and loss of personal data.

- Consumers lost £2.3bn during the Covid-19 pandemic as online fraud jumped by a third³.
- In the last year, online fraud and cybercrime has cost the UK more than £3bn (and the true figure may be much higher)⁴.

Cybersecurity has been ranked by the World Economic Forum as one of its five key global risks every year since 2012⁵.

73%

of UK organisations were affected by ransomware attacks in 2021¹ 15%

estimated growth in cybercrime in next 5 years and...

\$10.5
trillion

...estimated annual cost of cybercrime globally by 2025⁶

The Opportunity

Boosting cybersecurity protects individuals, improves trust in organisations and makes key infrastructure more resilient.

The development and adoption of core technologies such as cloud security, machine learning, the Internet of Things (IoT) and big data is enabling better detection and mitigation of cyber threats.

Cybersecurity investment by businesses can **protect valuable personal data** and **bolster consumer trust**, as well as drive growth and establish a competitive advantage.

A 2022 report by the Department for Digital, Culture, Media, and Sport (DCMS)⁷ estimated:

- > The UK cybersecurity market **grew by** 14% in the last 12 months.
- The number of active cybersecurity firms in the UK increased 24% in the last 12 months.
- > There are now **over 50,000 full time employees** working in the cybersecurity sector, an increase of 13% in the last year.

The UK's cybersecurity sector is now worth £10.1bn⁷.

Businesses are attracting record levels of investment: over £1.4bn was raised across 108 deals in 2021.

Areas of opportunity are emerging right across the cybersecurity value chain:

- >>> Research & Development
- >>> Distribution
- >>> Reselling
- Managed Security
 Services & Consultancies
- >> Training & Awareness

As our digital systems become ever more complex – and the threats to them ever more sophisticated – there is a growing demand for cybersecurity solutions that can make organisations more resilient and better protect people's personal data, financial assets, and reputations.



Business solutions

We are seeing a number of innovative businesses emerge across the value chain and within a range of sub-sectors, from Identity and Access Management (IAM) solutions to cybersecurity awareness training, attracting significant institutional investment.

IDENTITY

SOLUTIONS

SECURITY

MOBILE

ESTING

DING

GET IN TOUCH

The Bridges Sustainable Growth Funds invest in ambitious growth companies that are helping to build a more inclusive and sustainable

We would love to talk to businesses that are developing new cybersecurity solutions about how we can help them accelerate their growth and optimise their impact.

Please drop us a line via kyle.bentwood@ bridgesfundmanagement.com

BRIDGES

« NOTABLE SUB-SECTORS — VALUE CHAIN » —

IAM is a framework facilitating the management of digital/ electronic identities.

It reduces vulnerabilities relating to passwords and system access across devices, and allows IT managers to control access to sensitive information, for example via:

- Multi-factor authentication (MFA) requires approval via a second device to authenticate a login attempt.
- Single sign on (SSO) provides users a single point to log in and access all their applications.
- Privileged access assigns users different levels of access. Cloud-based IAM is a particularly high-growth segment, estimated to be growing at 30%+ per annum.

Demand is driven by the increase in remote/multi-location working methods and **growing risk of access to systems** via mobile devices/tablets.

These don't have the same level of built-in security capabilities as company devices, and so act as a 'back door' to business networks when connected. Many store enormous amounts of sensitive personal information.

• Mobile device management (MDM) and mobile threat defense (MTD) solutions keep device networks and data access secure.

Many individuals and organisations don't know where to start when it comes to cybersecurity. Many lack resources and struggle to convey the importance of cybersecurity to a non-technical audience.

Awareness training and testing educates across cyber threats and can be the difference between huge reputational and/or financial damage.

- Phishing threats are one of the most common and effective forms of cyber attack; 50% of people use the same password for all their logins (LastPass).
- Typical awareness training products include security awareness training courses & 'trial run' simulated attacks.

INVEST & DEVELOP

Software vendors invest heavily in tech **R&D**, developing core software products that are used to enhance cybersecurity across various sub-sectors.



EXAMPLE: OKTA

- US-based listed business, focused on cloudbased Identity Access Management
- · Six acquisitions in its lifetime; expected annual growth of 35%+ over next three years
- IPO'd in 2017; previously backed by Sequoia, Andreessen Horowitz et. al.

DISTRIBUTION

A core focus of software vendors is on product. For example, over 50% of Microsoft software sales are direct to the end user.

• IT Channel is critical in bringing products to market, providing local knowledge & access to customers, and educating customers on product benefits.

EXAMPLE: DISTOLOGY

- End-to-end distributor of cybersecurity products in UK and Europe
- Increased year-on-year revenues by 75%+ from 2018-2021; backing from Northedge in 2021

TRAINING & AWARENESS

Training services for IT staff or general workforce/individuals at risk; increasingly technology-driven, incl. simulated attacks.

EXAMPLE: KNOWBE4

- US-based business; provides automated tool allowing IT professionals to build customised security awareness programmes
- IPO'd in 2021; previous backing from KKR



MANAGED SECURITY SERVICES & CONULTANCIES

Given in-house cyber expertise is rare, outsourced **managed service providers** (MSPs) play a key role in providing effective cybersecurity functions and resilience 'penetration' testing.

EXAMPLE: QUORUM CYBER

- Managed detection and response services with global customers; a Microsoft Gold Partner
- Revenue trebled from May 2020-2021
- Backed by Livingbridge and Maven





Resellers own the relationship with end customers, providing a range of solutions, technical know-how and billing support. They often provide installation support and can provide managed services.



INVESTING IN THE FUTURE THE FUTURE OF INVESTING

ABOUT BRIDGES

At Bridges, we believe that investing in a better future for people and planet is both a moral imperative and an economic opportunity. By reducing our impact on the planet and helping more people to achieve their potential, we will boost productivity, reduce climate risks and foster new high-growth industries – creating lasting economic value.

We focus specifically on four themes, all of which are closely aligned with the Sustainable Development Goals:



Healthier Lives Solutions that improve physical and mental health and well-being



Sustainable Planet Solutions that help reduce emissions and decarbonise the economy



Future Skills
Solutions that
help people
to fulfil their
potential by
up-skilling or
re-skilling



Stronger Communities Solutions that improve access to quality goods, services and opportunities

