discribe

Digital security by design: opportunities, adoption, developer readiness, regulation and attitudes

Evidence from the Discribe DSbD Social Science Hub+

March 2025

Better digital security **protects** companies' valuations, **provides** competitive advantages and **unlocks** economic opportunities

Adoption won't be driven by the market alone but can be encouraged by appropriate **regulation**

Developers and programmers need **clear documentation**

Collaboration beyond technical and organisational **silos** is essential to overcome barriers to widespread adoption of digital security by design

This report captures evidence and insights from Discribe's interdisciplinary, applied research and Futures programme. It provides a forward-looking analysis, including geopolitical aspects, emerging questions and practical implications.

'Discribe brings diverse thinking together to help realise the possibility of a secure digital future for all, and we believe we can transform policy making, accelerate adoption and drive consistent use.'

– Adam Joinson
Director of Discribe Hub+

Contents

A digital society needs **stronger foundations**

The infrastructure underpinning digital computing is inherently insecure. The digital world delivers huge opportunities and benefits to societies and people, and every year we're more dependent on it and connected to it. But today's computer systems face significant challenges in data security and protecting operations. Memory safety issues lead to software vulnerabilities that can be exploited by attackers.

The **Digital Security by Design** (DSbD) programme brought together partners from leading technology companies, academic institutions and UK Government agencies to develop systems and software implementations to address system vulnerabilities. Discribe is the Economic and Social Research Council (ESRC) DSbD Science Hub+ and part of the DSbD programme.

DSbD

- set up in 2019
- collaboration between the UK Government, academia and industry to deliver a more secure, resilient and trustworthy digital world
- has been delivered through £80m of UK Research and Innovation (UKRI) funding matched by more than £200m of industry co-investment

Discribe

- launched in 2020 following an open competition
- community of social scientists, economists, computer scientists and arts and humanities professionals
- £3.5m funding to conduct and commission research into the social and economic barriers to next generation digital security success
- partnership between four universities: Bath, Bristol, Cardiff and Royal Holloway, University of London

CHERI and Morello: Transforming memory safety and security

DSbD has developed a hardware and software ecosystem using CHERI and Morello technology to make processors more robust and able to deter security breaches:

- **CHERI** (Capability Hardware Enhanced RISC Instructions), designed by the University of Cambridge and SRI International, introduced memory protection and compartmentalisation to address vulnerabilities caused by bugs and programming mistakes. 70% of known operating system cyber security vulnerabilities are due to memory safety issues.[1]
- The **Morello Board** is a high-performance technology platform prototype, built by Arm Ltd using CHERI and Morello and Sonata technology prototype. The **Sonata Board** is an open-source development board, available through lowRISC and Microsoft.
- **DSbD's Technology Access Programme** enabled companies and universities to experiment with the Morello board, distributing around 500 boards.
- CHERI was technically proven. The DSbD programme also found evidence[2] that **CHERI**
  - **reduces business costs**
  - **enhances user and developer experience**
  - **strengthens digital security and resilience**

[1] National Cyber Strategy (2022)

[2] Read the evidence

Discribe at a glance

From smarter cities to secure shopping, protected healthcare records to thriving small businesses – when our data is safe, we can innovate and unlock inclusive economic growth. But more secure technology will have no impact unless we use it. Discribe was established to explore issues around the:

Adoption of new technologies

Work package (WP) 1, led by the University of Bath

Readiness of software engineers to code for CHERI

WP2, led by the University of Bristol

Regulatory and policy implications of CHERI

WP3, led by Royal Holloway, University of London

Potential differences across industrial sectors and parts of society in attitudes towards digital security by design

WP4, led by the University of Cardiff

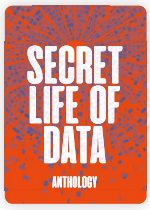
Discribe also ran the Futures programme

which used creative engagement techniques to bring together diverse stakeholder groups, stimulate dialogue and imagine possibilities

£1m fund to commission research

19 universities – four core partners and Aston, Birkbeck, Cambridge, Coventry, Delft, Essex, Leicester, Manchester, Newcastle, Northumbria, Nottingham, Oxford, Sheffield, UEA and Warwick

More than **16** other partners, including Airbus, HSBC Bank Plc, Katlas, Microsoft, Mindhug, RSA Security



200+ submissions to "Secret Life of Data"

57 researchers funded across **24** core and commissioned projects

Over **1000** participants at nine DSbD events run by Discribe to share information and develop the ecosystem

40+ documents published: reviews, games, papers, reports and a short story collection

Over **167,000** views of a Reddit 'Ask Me Anything' event which included Discribe researcher Dr Oishee Kundu

Discribe research reveals that:

- better digital security:
  - **protects companies' valuations** (page 6)
  - **provides competitive advantages** (pages 6, 7)
  - **unlocks economic opportunities** (pages 6, 7, 8, 15, 16)
- **adoption** won't be driven by the market alone but can be encouraged by appropriate **regulation** (pages 10, 11, 14-17)
- developers and programmers need clear documentation or risk 'floundering' (page 12)
- **collaboration beyond** technical and organisational **silos** is essential to overcome barriers to widespread adoption of digital security by design (pages 13, 17)

Discribe outputs to date

Discribe conducted core research and managed a commissioning fund for scoping reviews, 'Connecting Capabilities' and 'Actionable Insights' research.

Through Discribe, researchers and businesses contributed to a better understanding of how digital security hardware will be used, what the barriers to that use might be and how these can be overcome.

- More than **34 papers** based on Discribe researchers' work have been accepted for publication in peer-reviewed journals and conference proceedings.
- Discribe's community of practice have:
  - participated in **panel discussions** (including at the Cheltenham Literature Festival)
  - developed **physical and online resources**
  - given **evidence** to the McPartland Review of cyber security and economic growth and to the UK Government Science, Innovation and Technology Committee's Inquiry into cyber resilience of the UK's critical national infrastructure
  - presented to **conferences** including the International Conference on Industry Science and Computer Sciences Innovation, the International Naturalistic Decision Making Conference and the British Academy of Management Conference
  - hosted regular Cyber Tuesday **networking sessions** for TechSpark
  - convened or participated in **working groups** with ARM, the Department for Culture, Media and Sport, Digital Catapult, the Engineering and Physical Sciences Research Council, the ESRC, IoT Horizon, Innovate UK, SEMI Europe, UKRI and other stakeholders
  - participated in **DSbD roadshows**
  - engaged with other **UKRI networks,** including SPRITE+ and the Research Institute for Sociotechnical Cyber Security

This report highlights insights from the Discribe research teams. It:

- addresses the economic and societal cases for security with insights from our research
- highlights key findings by theme: adoption, readiness, regulation and policy, and cross-cutting attitudes
- signposts how Discribe's Actionable Insights projects, including two games and a cost-benefit simulator, are enhancing understanding of incentives to adoption
- shares outputs of commissioned work, including the 'Digital Sovereignty by Design' project, which aimed to identify impacts that the EU's move to digital sovereignty present for the UK's cybersecurity landscape; and the expansion of the CHERIoT programmers' guide
- reveals insights from Discribe's Futures programme
- considers the implications of 'shifting sands', a fast-evolving international political and economic environment and forthcoming domestic developments on digital security
- reflects on the value social science adds to technical and scientific research programmes

Access papers and other documents published by Discribe researchers

The **economic case** for digital security by design

The expansion of cyberspace has changed how we live, work and communicate. It is transforming the critical systems we rely on in areas including finance, energy, food distribution, healthcare and transport, and is 'integral to our future security and prosperity' (UK National Cyber Strategy).[3]

This offers **"extraordinary opportunities"** for the UK to pursue national goals in new ways, the Strategy notes, but has unleashed 'unprecedented complexity, instability and risk'.

The UK is one of the world's leading digital economies and a top five nation in innovation, artificial intelligence (AI) and cyber, well-positioned to harness the transformative effects of science, technology and digital to drive innovation and business growth. These strengths bring risks:

- The Department for Science, Innovation and Technology (DSIT) Cyber Security Breaches Survey covers the prevalence and impact of breaches and attacks.
- The Government notes that technology advances **increase** the ability to threaten and damage countries, societies and individuals remotely and anonymously and 'the use of commercial spyware, ransomware and offensive cyber capabilities by state and non-state actors has proliferated.' This 'highlights the importance of engaging with technology companies and shaping responsible norms of behaviour' with respect to cyberspace and technology.

The McPartland Review[6] recognised the **need to collect evidence** to drive cybersecurity as a facilitator for digital transformation. **Discribe researchers studied the economic impact of cybersecurity** within the contexts of the work packages. Findings include:

- Cyber security breaches have a negative impact on stock market valuations, according to a systematic literature review by Covachev, Syrda & Joinson.[7] his effect is particularly pronounced for organisations in the financial sector. Breaches in one firm can have **negative or positive effects** on other firms in the same industry through contagion or customer switching. The Discribe researchers' (unpublished) review is consistent with findings published by Ali, Lai, Brown, Lowry and Ali,[8], who found that the magnitude of stock market reactions to cyber-attacks and information security event announcements are contingent on time frame, industry type, breach type and firm size.
- Discribe researchers from the Universities of Essex, Greenwich and Loughborough surveyed 239 small and medium-sized enterprises (SMEs). Their findings[9] demonstrate, firstly, the 'myopia' of many SMEs to cyber threats, secondly, that cyber security capabilities should be viewed as organisational capabilities, with **increased security and resilience providing competitive advantage** to firms: 'The effectiveness and strength of an organisation's cybersecurity capabilities directly influence its overall performance.'[10]

[3] National Cyber Strategy (2022)

[4] 'Integrated Review Refresh 2023: Responding to a more contested and volatile world', (2023) HM Government.

[5] ibid

[6] McPartland review of cyber security and economic growth: terms of reference

[7] Covachev, Syrda & Joinson (2021) Draft review: Stock market impact of breaches

[8] S. A. E. Ali et al. (2021) 'Stock market reactions to favorable and unfavorable information security events: A systematic literature review', *Computers & Security*.

[9] J. C. Fernandez de Arroyabe et al. (2023) 'Cybersecurity Resilience in SMEs. A Machine Learning Approach', *Journal of Computer Information Systems*.

[10] ibid

- Within Discribe WP1 (page 10) Lam and Seifert studied determinants of firms' secure hardware adoption decisions in the context of Open Banking and related Open Data markets, in which sharing consumer data between firms 'can generate substantial economic benefits'. The findings[11] of their game-theoretic approach show that adopting secure hardware reduces the probability of successful cyber-attacks, **which reduces liability costs for firms**. Their work, which also draws on interviews with stakeholders in the technology, finance, energy and local government/regulatory sectors, shows that investing in security enables firms to **participate** in Open Data schemes and facilitates innovation – both of which can increase market share. They reported that super-compliance can **give firms a competitive advantage** (but this depends on the extent to which security advantages can be effectively marketed).
- It remains difficult to quantify the likely cost of a breach to an organisation, and while variables such as time to recover are helpful they do little to quantify reputational or social damage. But Lam and Seifert find vulnerabilities in critical sectors like energy and banking can decrease confidence and have wide negative effects across the economy.
- Models for deciding optimal levels of investment ('good enough') in security are becoming more sophisticated and often incorporate aspects of threats faced, assets to be protected and effectiveness of security functions. However, they often operate in silos and fail to capture the complexities of real-world decision-making:
  - A Discribe researcher is studying how these models simplify decision-making processes. A preliminary review of the data suggests they typically simplify the process, assuming cyber security investment strategies are universally applicable. However, real-world environments are dynamic, shaped by diverse organisational, technical and regulatory factors that normative approaches often exclude.
  - Existing models frequently fail to address the unique organisational and contextual challenges that influence cyber security investment decisions. They tend to rely on one-size-fits-all assumptions, neglecting industry-specific risks, organisational culture and external pressures.

One economic benefit consistently identified in our work is the **connection between digital security and the opportunities of digital transformation** amongst firms. Some evidence also pointed to **firms' reticence to embrace new digital technologies due to security concerns**.

- In a follow up study using Eurobarometer survey data of 3,180 manufacturing sector SMEs, the Essex, Greenwich and Loughborough team[12] noted that SMEs are incorporating digital technologies to **increase productivity** or because of supply chain requirements. They found that **IT security issues positively affect this digitalisation** and that digital transformation poses new security challenges that firms must address to fully exploit the new opportunities offered by, for instance, AI, smart contracts, etc.
- Lam and Seifert[13] also note that increased security might lead to more data sharing, and thus to a lower socially optimal outcome (if, for instance, that data sharing has a negative outcome for consumers). They conclude that **regulation that does not acknowledge the market and competition – and deals simultaneously with both security and data protection – could be counter-productive** (see also their briefing paper).[14]

[11] Secure Hardware Adoption in the Open Data Context

[12] The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges

[13] Secure Hardware Adoption in the Open Data Context

[14] Harnessing Market Incentives to Improve Cybersecurity Outcomes for Firms and Consumers

Gaming cyber security: how businesses weigh risks and investments

Organisations need to balance investment in security against other business development requirements. Discribe researchers at the University of Bath (Stsiampkouskaya, Joinson, Syrda and Kundu) developed a game (Threats and Trade-offs) to study these choices.

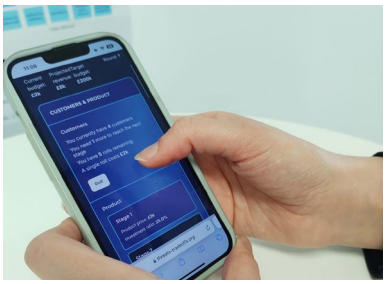
Game rules:

Players must try to grow a Smart Healthcare startup while fending off cyber-attacks.

Patient information is stored in the cloud and accessed by patients, doctors and employees.

Players must choose whether to invest in secure hardware (they can opt for a 'standard' reader device to send data to the cloud, or a DSbD device which costs two-and-a-half times more). They can also invest in a range of cyber defences.

As the game progresses and their startup expands, players make further choices about which hardware and defences to reinvest in.



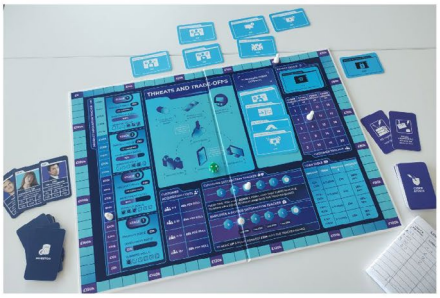
Key insights:

Data from **118 gameplays** across three gaming sessions reveals that the most common strategy (followed by nearly 40 % of participants) **is to choose not to invest in secure hardware**, with this decision not driven by funds.

Those games were characterised by high subsequent spending on cyber defences, the lowest customer satisfaction scores and the least profitability.

Players who started by choosing the standard reader were less likely to switch to the DSbD reader later, a classic case of 'technological inertia'.

Players who experienced a cyber-attack that they were unable to protect against were more likely to choose the 'secure by design' (DSbD) reader – but those who do not react by investing in the more secure reader are less likely to with subsequent breaches. This suggests that learning may play a larger role than recency bias in security adoption.



As above, a lack of security (and thus increased likelihood of a breach) has a financial cost for organisations in terms of market capitalisation and potential fines (for data loss). Other impacts (e.g., reputational damage, loss of intellectual property) exist but are more difficult to quantify. Quantifying return on investment in new security technologies remains difficult.

There is evidence of the opportunity costs of failing to adopt secure hardware and that enhanced security opens new opportunities through open data and open banking, and that new opportunities increase the likelihood of adoption via increased vulnerabilities (Lam and Seifert). Attempts to 'nudge' adoption must also recognise the danger of over adoption and the potential to create less than socially optimal outcomes (e.g., by encouraging data hoarding).

The **societal case** for digital security by design

The UK National Cyber Strategy (2022)[15] argues for a 'whole-of-society' approach to cybersecurity, with security and resilience the responsibility of government, industry and third sector organisations.

The government's 'Cyber Security Strategy: 2022 to 2030' describes how increasing digital connectivity, and the better use, generation and organisation of data, will offer the government significant opportunities to improve services and functions, to benefit the UK and its citizens. Digital transformation will drive innovation, scaling up capabilities and understanding.[16]

Discribe has not commissioned or conducted research on the societal case for security. However, in the course of our work we have identified the following challenges:

- a lack of security (or in-built vulnerabilities) can be seen as an externality wherein cost is transferred from source to end user
- end users may make complicated calculations when balancing trade-offs between the potential costs of adoption in secure technology compared with the consequences of a breach or cyber-attack and any potential performance loss
- in the local authority context, data losses can expose particularly vulnerable members of society to harm (Lam and Seifert)[17]
- security could be viewed as a 'public good' (like clean air), requiring governmental intervention and support

These challenges should be investigated in more depth.

Discribe's DSbD Futures programme (page 18) examined the extent to which positive ('utopian'), negative ('dystopian') and business-as-usual ('BAU') consequences of DSbD are 'plausible, possible and preferred'. Some of the positive consequences imagined included:

- an 'unhackable' integrated GOV.UK portal with greater automation, speed and efficiency
- next generation integrated Internet of Things (IoT)
- personal care/healthcare robotics
- home surveillance

Many of the story stem submissions from IT experts and non-experts in large organisations (page 15) and stories from the public submitted to our creative writing book (page 18) imagined future societal opportunities or consequences resulting from strong or poor digital security. Views of the future can be seeded by societal and individual perceptions which are typically 'extensions of the present' which can risk chronocentric 'blind spots' (Liveley and Coles-Kemp).[18]

Discribe demonstrates the **importance of thinking beyond 'BAU'** (page 17), and of balancing measures that enable innovation with others that may not be economically justified but protect what we consider to be of public value or benefit. However, what is of benefit to one community may be detrimental to another (Liveley and Coles-Kemp).[19]

[15] National Cyber Strategy (2022)

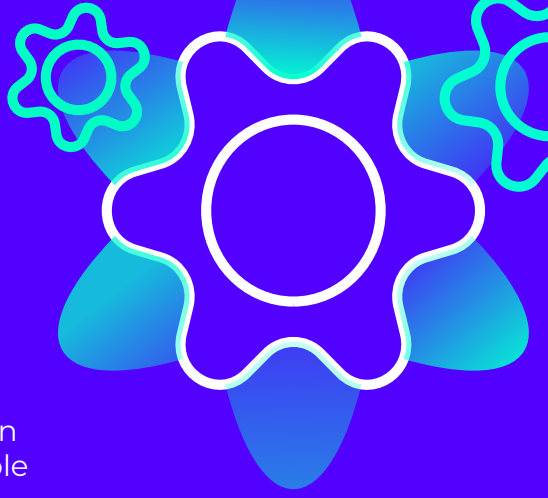
[16] Government Cyber Security Strategy (2022–2030)

[17] Secure Hardware Adoption in the Open Data Context

[18] G. Liveley and L. Coles-Kemp (2022) 'Futures'.

[19] ibid

Barriers and challenges to **adoption**



Key findings:

Discribe offers multiple sources of evidence that adoption is unlikely to be driven by customer demand, new secure-by-design technologies need to be priced competitively with relatively stable supply chains, and compliance with regulation or standards is likely to be the strongest driver of adoption. A 'build it and they will come' approach will not be a sufficient driver of the adoption of DSbD technology.

A large proportion of Discribe's research focused on barriers to and enablers of secure technology adoption (WP1).

In their Discribe-funded scoping review 'Drivers and barriers for secure hardware adoption', Tomlinson, Parkin and Shaikh (2022)[20] outline the factors commonly associated with adoption of security technologies, including enhanced security (and subsequent avoidance of harms from breaches) and market-led demand (when customers demand improved security).

- They identified technical and skills barriers (in particular, around hardware security), increased costs and potential issues in the hardware supply chain as barriers or challenges to adoption.
- Through interviews with technical stakeholders, Tomlinson et al. identified compliance, standards and regulation as consistent motivating factors for adoption of DSbD technologies, across industrial sectors, with mixed views (and some scepticism) that market forces would drive adoption.
- They worked with the global semiconductor association, SEMI, and industry association TechWorks UK to recruit cross-sector interviewees. Interviewees also expressed concern around potential skills issues with new secure hardware, and the integration of new technologies within existing systems. An additional barrier mentioned was the difficulty measuring the benefits of adoption of more secure technologies.

In a survey study of 76 IT and security professionals:

over **70%** selected **regulatory requirement as the most likely incentive for adoption of DSbD technologies**

with **63%** also concerned about competitive pricing

There was more support for mandating manufacturers to include DSbD technologies in their devices (78%) than for end user adoption to be mandated (67%).

Additional interviews as part of a Discribe-funded review by Benson et al.[22] found that **adoption is unlikely to be driven by demand**, and that even when compliance is enforced through procurement (e.g., via Cyber Essentials compliance) this may not translate to widespread awareness or adoption.

A cost-benefit simulator[23] built by Shaikh and Mudassir **allows users to assess the benefits of adopting CHERI-based technology, assessing return on investment and potential cost savings**. It covers the automotive, semiconductor, airline, clothing and retail industries.

[20] A. Tomlinson et al. (2022) 'Drivers and barriers for secure hardware adoption across ecosystem stakeholders', *Journal of Cybersecurity*, 8(1), tyac009.

[21] S. Furnell et al. (2023) 'Assessing Organizational Awareness and Acceptance of Digital Security by Design', *Journal of Information Systems Security*, 19(1), pp.3–18.

[22] V. Benson et al. (2021) 'Regulation, Policy and Cybersecurity: Hardware Security'.

[23] Cost-benefit Simulator for Hardware-based Cybersecurity

Initial findings from data collected through Threats and Trade-offs, a game-based simulation, are covered on page 8, with analysis of over 100 game-plays demonstrating some 'technological inertia'. CyberQuest is another Discribe-funded simulation game, developed by the University of Essex and designed to help managers integrate cybersecurity best practices and adopt new digital technologies effectively. Beta testing of CyberQuest is underway. Both games could subsequently be adopted by firms and within higher education curricula.

Sector-specific adoption studies

The research by Benson et al., conducted between February and July 2021, focused on regulatory frameworks in the UK digital sector (pages 14–16). It explored the automotive and fintech industries. Both are dependent on secure IT systems; in both, technology is advancing faster than regulatory efforts. **Adoption (of digital security by design technology) could come through standardisation or self-regulation, not only regulation.**

Fintech and financial services

Benson et al. noted a lack of harmonisation of hardware security standards and highlighted 'pervasive contradictions across standards and legislation' in financial services (FS) and the fintech industry. While fintech is highly compliance driven, with an ingrained acceptance that meeting regulatory needs is a 'cost of doing business' that helps to avoid loss, compliance is driven by the principle of 'good enough' security and a rudimentary cost-benefit analysis. Furthermore, FS and fintech are not governed by a single regulatory framework in the UK: firms involved in consumer credit, banking and advising on investments are authorised and regulated by several bodies.

The research suggested that hardware security innovations in fintech are often deprioritised in favour of faster time-to-market or cost considerations. **Successful adoption of DSbD technologies would require engagement with industry associations, regulatory bodies, and government agencies to integrate these solutions into existing regulatory frameworks around hardware assurance levels and security by design.**

Automotive

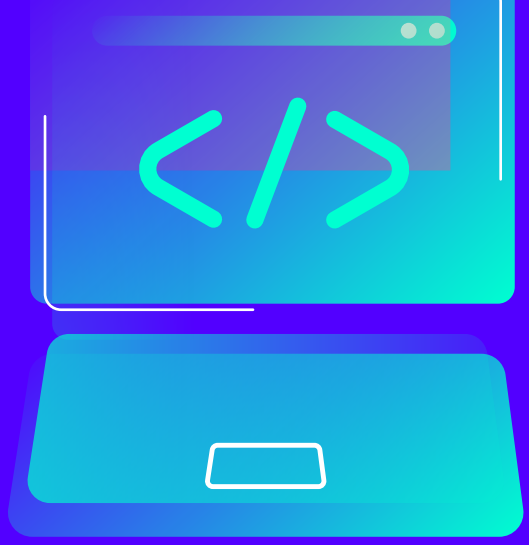
Benson et al. described worldwide efforts to improve automotive security (including vehicle cyber and hardware security), highlighting legislation, regulation, standards and guidance (some of which was due to come into effect from 2022 onwards). **They noted that the UK government's principles 2, 4 and 5 for automotive security (focusing on risk assessment, supply chain security and security by design) would collectively support the adoption of DSbD initiatives.**

Their research also highlighted that the threat of cyber-attacks is particularly relevant for Connected and Autonomous Vehicles (CAVs), describing multiple attack types, vectors and surfaces: the transition to CAVs could drive adoption of DSbD approaches.

Software developer **readiness**

Key findings:

Developers and programmers require simple, clear documentation. Technical specialists, manufacturers and users are siloed, as are organisational self-assessment methodologies – an integrative approach is needed.



WP2 ‘Readiness’ examined software engineers’ and developers’ readiness to work with new secure hardware.

Bristol Cyber Security Group’s evidence[24] to the Government’s inquiry into the cyber resilience of the UK’s critical national infrastructure called for recognition of the importance of security awareness and training among software developers, security engineers and architects. This would ensure that ‘secure by design is a philosophy across the socio-technical system and not merely a technological consideration’.

Hallett, Alhindi and Shreeve sought to identify what issues developers may face when porting their software to CHERI’s architectures.

- They observed a panicked ‘guess and hope’ approach when developers working with CHERI code were presented with an error message or code they did not understand. Hallett et al. created a new code smell,[25] ‘floundering’ to reflect this behaviour.
- Their research participants also found the ‘Introduction to CHERI and CHERI C/C++ Programming Guide’ intimidating, long and hard to read; Hallett et al. suggest simpler and more focused documentation for developers who just want to work with CHERI without understanding its full features and security architecture.
- Discribe subsequently funded David Chisnall (SCI Semiconductor; Visiting Professor, University of Cambridge Computer Laboratory) to develop the CHERIoT Programmers’ Guide through our ‘Making CHERI usable’ call (page 19).

Ullah and Rashid sought to identify potential developer-induced vulnerabilities and compiler limitations as Morello navigates towards market induction. Their paper[26] showed that **despite Morello’s advanced security features, some developer-induced vulnerabilities remain exploitable**, emphasising the importance of adhering to established programming standards like CERT guidelines.

[24] Written evidence submitted by the Bristol Cyber Security Group’ (CYB0035). Available here.

[25] Useability code smells for programmers include poor documentation and confusion about warnings. N. Patnaik et al. (2019) ‘Usability Smells: An Analysis of Developers’ Struggle with Crypto Libraries’, in ‘Fifteenth Symposium on Usable Privacy and Security’ (SOUPS 2019), pp.245–57.

[26] S. Ullah and A. Rashid (2024) ‘Porting to Morello: An In-depth Study on Compiler Behaviors, CERT Guideline Violations, and Security Implications’, 2024 IEEE 9th European Symposium on Security and Privacy (EuroS&P), Vienna, Austria, pp.381–97.

Breaking out of silos

Slesinger, Coles-Kemp, Panteli, and Rydhof Hansen[27] demonstrated that **hardware security engineers, software engineers and coders, manufacturers in the technology supply chain and end users exist in siloed communities** and proposed an integrative approach to security design.

Furnell, Bada and Kaberuka showed that the concept of DSbD is generally unknown to non-technical professionals.[28] Organisational 'DSbD readiness' is dependent on multiple perspectives across different parts of a business, rather than being the sole responsibility of those with technical roles including chief information security officers and chief information officers.

Furnell and Bada's 2024 report, 'Assessing Organisational DSbD Awareness and Readiness', presented their work to develop and test a prototype Self-Assessment Tool (SAT) for organisations to assess their own DSbD readiness. They captured multiple perspectives from stakeholders including business and technical leaders, to understand alignment around security priorities and potential adoption of secure-by-design approaches. Their SAT could be integrated with existing assessment frameworks, they suggest.

[27] I. Slesinger et al. (2022) 'Designing Through The Stack: The Case for a Participatory Digital Security By Design', in 'New Security Paradigms Workshop' (NSPW '22), October 24–27, 2022, North Conway, NH, USA. ACM, New York, NY, USA, 15 pages.

[28] S. Furnell et al. (2023) 'Assessing Organizational Awareness and Acceptance of Digital Security by Design', *Journal of Information Systems Security*, 19(1), pp.3–18.

The **legal and regulatory** opportunities for digital security by design

Key findings:

Discribe evidence suggests that appropriate regulation will be necessary to drive adoption of digital security technologies. A co-ordinated and joined-up approach to regulation (and compliance and trust frameworks) may address market failures, incentivise adoption and enable opportunities.

WP1 **'Adoption'** (pages 10–11) revealed that compliance with legal or regulatory requirements is the strongest driver of adoption of new security technologies (and indeed policies). WP3 '**Regulation**' examined this in detail with Discribe also commissioning research in this area (pages 15–16). The work sought to uncover **regulatory challenges** emerging from new DSbD technologies and examine cultural, social, and organisational factors that may influence the regulatory landscape of the new security hardware.

An initial review[29] by Benson et al. (pages 10–11) found progress has been made in legislation, standards and regulation for hardware security, but that policy makers' approaches have been disconnected. Their work identified **common weaknesses** including low use of secure mechanisms that are available, a lack of adherence to good practice in system design and a lack of tamper detection capability. Industries which are experiencing exponential technological dependencies often have multiple regulators and it is complicated and complex to develop hardware standards.

Slesinger, Panteli and Coles-Kemp identified **four perspectives in how regulation is perceived by DSbD programme stakeholders:** as an ethical imperative, to add value to products and services, as a lever for adoption, and as a regime to be passively complied with.[30] A key finding was **the importance of relationship-building and dialogue between stakeholders** to establish and implement the regulatory environment and requirements around CHERI.

Data leakage and security vulnerabilities are serious concerns in healthcare. In the UK, nearly eight out of ten healthcare providers have experienced at least one data breach since 2021. At least 80% of health apps – many trusted and recommended by the NHS – don't meet security and privacy standards.[31] Discribe funded the development of a data structure model showing how CHERI/Morello would protect different types of patient data (identification, journey and treatment). Discribe researchers from Royal Holloway University of London and Queensland University of Technology examined how CHERI/Morello technologies could support a medtech start-up's Licensed Healthcare Software service design.

---

[28] S. Furnell et al. (2023) 'Assessing Organizational Awareness and Acceptance of Digital Security by Design', *Journal of Information Systems Security*, 19(1), pp.3–18.

[29] V. Benson et al. (2021) 'Regulation, Policy and Cybersecurity'.

[30] L. Slesinger et al. (2024) 'Regulating Digital Security by Design? Implications of the Perspectives from DSbD Programme Stakeholders', *Information and Computer Security*, 32(5), pp.676–90.

[31] Organisation for the Review of Care and Health Apps (Orcha). Multiple authors in academia and industry have investigated the safety, security, transmission and encryption of data in widely-used health apps. For example, a literature review of privacy protections and data ownership in mobile health (mHealth) technologies between 1 January 2016 and 1 June 2019: H. K. Galvin and P. R. DeMuro (2020) 'Developments in Privacy and Data Ownership in Mobile Health Technologies, 2016–2019', *Yearbook of Medical Informatics*, 29(1), pp.32–43.

Discribe researchers from Royal Holloway University of London and Queensland University of Technology examined how CHERI/Morello technologies could support a medtech start-up's Licensed Healthcare Software service design. Their research report[32] describes how implementing CHERI/Morello when developing products offers the start-up, MindHug, benefits including data assurance, better performance compared to cloud-based alternatives, future-proofing against emerging threats and meeting compliance requirements.

Burdon and Coles-Kemp defined a Digital Responsibilities Framework which consists of five types of responsibility actions along a spectrum, from full 'absorption' to refusing responsibility. The framework helped Heath, Burdon and Coles-Kemp to identify how Discribe collaboration partner Katlas, an early-adopter of Morello which has designed a Web 3.0 router with blockchain-enabled tools, mapped its data protection and security responsibilities, fully absorbing some, allocating others and 'refusing' others so they remain end-user responsibilities.

Lam and Seifert investigated the relationship between firms' data privacy and cybersecurity choices, identifying market failures ('firms tend to under-invest in security and over-share data') and studying regulatory interventions that may resolve these market failures. Their findings suggest that stricter oversight of firms' cybersecurity choices than is currently the case under the UK GDPR may be appropriate; and that a coordinated approach to regulation, which accounts for firms' interdependent data sharing and cybersecurity choices, is needed. More reinforcement comes from Discribe's evidence that cyber security breaches can cause 'contagion' or 'competing' effects (page 6), which can create misaligned incentives for businesses to participate in industry-level incident information sharing.

Panteli, Leach and Coles-Kemp[33] examined potential tensions that may arise between security innovations and security governance, indicating a tension between compartmentalisation (a key feature of CHERI) and the need for integration for security governance purposes which the researchers intend to explore further. They also highlighted that security governance involves both technological and administrative elements, with the latter encompassing policies, management structures and risk processes that go beyond purely technical considerations. Their study, based on interviews with cybersecurity leaders and other experts within the DSbD network, revealed another tension between the need for organisational agility and the constraints or 'locking in effect' of new digital security systems.

Geopolitical aspects of digital security by design

Discribe-commissioned 'digital sovereignty by design' research underlines the interdependencies of digital security and economic opportunity: 'Trade and economic security affect cybersecurity as much as cybersecurity affects trade and economic security…economic goals are security goals, and vice versa. Achieving both is dependent upon, and in turn reinforces, sovereignty.'[34] Again, this emphasises the role regulation will play in adoption and the need for collaborative work.

EU technology policies are increasingly influenced by concerns of strategic autonomy with regulatory interventions framed in terms of 'digital sovereignty.' Farrand investigated the semiconductor supply chain lifecycle, from raw materials through manufacturing to end-use. Security is central to every part of the supply chain and is realised through economic means that seek to boost industrial production in Europe.

[32] C. Heath et al. (2024) MindHug & CHERI/Morello, Discribe/DSbD report on Licensed Healthcare Software.

[33] N. Panteli et al. (2024) 'Compartmentalization Vs Integration: Tensions Between Digital Security Innovations and Security Governance'. ECIS 2024 TREOS, 48.

[34] B. Farrand et al. (2024) 'The new geopolitics of EU cybersecurity: security, economy and sovereignty', *International Affairs*, 100(6), pp.2379–97.

Economy and security are not distinct policy areas, but interlinked, interdependent and 'essential for the EU's continued survival in the face of geopolitical instability'.

Carrapico and Farrand[36] analysed developments in EU cybersecurity policy during 2023 covering varied legislative initiatives, including the directive on measures for a high common level of cybersecurity across the Union (Directive 2022/2555, also known as NIS2) which seeks a more joined-up, collaborative and consistent approach and stronger 'oversight and enforcement'.

They conclude that this directive, along with proposed modifications to the Cybersecurity Act, the proposal for the Cyber Solidarity Act, the Cyber Resilience Act and the Institutional Cybersecurity Regulation (Regulation 2023/2841), all reflect a '**regulatory mercantilist**' frame of heightened oversight and regulatory hierarchy, moving from narrower confines (setting private sector obligations) to an all-encompassing cybersecurity framework.

The Cyber Resilience Act will require hardware and software products available in the EU to be cyber secure throughout their life cycles and for consumers to be given sufficient information about products' security to make informed choices. It will give the European Commission market surveillance and enforcement powers and is framed as allowing Europe to 'reap all the benefits of the digital age and to strengthen its industry and innovation capacity, within safe and ethical boundaries'. Carrapico and Farrand suggest standards developed through EU regulation could be exported to the international arena to cement the EU's position as a global leader.

Farrand, Carrapico and Turobov[37] return to semiconductors and two legislative initiatives, the Chips Act (2023) and the Critical Raw Materials Act (2024), in 'The New Geopolitics of EU Cybersecurity'. Communication around the Chips Act argued that 'European leadership in the semiconductor industry is essential for the EU's economic competitiveness, as well as its technological sovereignty and security'. The Critical Raw Materials Act seeks to ensure access to a secure, resilient and sustainable supply of the critical raw materials for semiconductor manufacturing, framing this, along with legislation concerning the locations of data servers, as reducing dependencies and critical in the face of an uncertain geopolitical environment and potential – and perceived – technological vulnerabilities.

[36] H. Carrapico and B. Farrand (2024) 'Cybersecurity Trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics', *Journal of Common Market Studies*, 62. Annual Review pp.147–58.

[37] B. Farrand et al. (2024) 'The new geopolitics of EU cybersecurity: security, economy and sovereignty', *International Affairs*, 100(6), pp.2379–97.

Across **contexts**

Key findings:

Attitudes are diverse, reflecting how different sectors, groups, communities and individuals have varied priorities, knowledge, power and risk exposure. Research within this WP provides additional evidence supporting Discribe's findings that appropriate, fit for purpose regulation is necessary to drive adoption, and of the need to collaborate beyond silos.

WP4 'Across contexts' explored potential differences in attitudes towards digital security by design, across industrial sectors and society. The research investigated factors that influence the propagation of opinions around:

- technology adoption, resistance and perceptions of risk
- differences between online narratives and behaviours
- relationships between public policy on cybercrime reduction and stakeholder perception, and between the regulatory landscape and the uptake and adoption of cybercrime prevention mechanisms by business

A review by Sanger, Gore, Foster, Zamani, Gamblin and Dale of 66 articles, examining the adoption of new security technologies, identified four categories of benefits (reputational, financial, risk-related and compliance-related) and four categories of risks (technological, organisational, environmental and human/actor-related). It demonstrates the importance, especially to businesses, of the **need for a holistic approach to adopting new security technologies, requiring consideration of technological**, organisational, environmental and human/actor-related risk factors, with no one factor focused on to the exclusion of others: 'technological risks and decisions are not more important than organisational, human or environmental ones.'[38]

The second report of Sanger et al.,[39] from their 15-month Discribe project, covers the perceptions and behaviour of IT experts and non-experts in large organisations. Using a 'story stem' methodology, the researchers collected and analysed 454 brief stories about fictional situations regarding cyber security adoption in the workplace. They also investigated security adoption in higher education.

Four key themes in attitudes toward security adoption emerged in the stories: accountability (and blame), emotional responses (particularly fear and stress around security incidents), cynicism/negativity (especially regarding management's handling of security) and concerns about reputational impacts. IT experts showed more positive attitudes and focused more on socio-technical aspects compared to non-experts, who emphasised blame and negative outcomes; this highlights the importance of senior management teams trying to reduce 'organisational cynicism' of cyber security.

[38] S. Sanger et al. (2023) 'Understanding the Security Technology Adoption Process: A Rapid Evidence Review'.

[39] ibid

The research into higher education revealed insufficient interest in cyber security by their boards of trustees. It was often seen as a lower priority than other risks. But higher education institutions (HEIs) were more likely than businesses to have technical controls in place conforming to 'Cyber Essentials' requirements (e.g., firewalls, secure configurations, user access controls, malware protection and software patch management); more likely to seek out advice when needed; and more likely to take action to identify cyber security risks than businesses. However, half of the HEIs surveyed had gaps in supply chain oversight relating to security.

Social media platforms play a significant role in facilitating business decision making, especially in the context of emerging technologies, and research by Williams, Anthi and Burnap[40] sought to identify key factors which maximise the impact of emerging technology-related tweets.

They found tweets expressing negative sentiments were more likely to be impressionable, potentially due to the negativity bias where such content elicits stronger emotional responses, thus driving higher engagement and virality. However, positive sentiments associated with technologies perceived as beneficial (e.g., data science, machine learning) significantly contributed to tweet impressions.

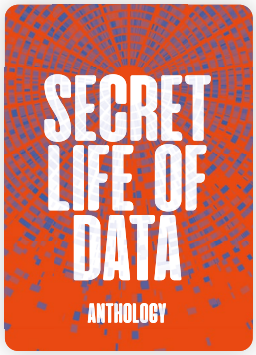
The Temporal Network Analysis by Williams, Khan and Burnap[41] demonstrates the adaptive nature of the DSbD ecosystem, offering insights about shifts in focus, emerging trends and evolving relationships between 2019–2024. Key findings include the increasing centrality of 'trust' and 'AI' in discussions, reflecting the growing integration of AI into digital security strategies which the researchers expect to grow. They anticipate more collaboration between government agencies, industry, academia and international bodies (and more cross-border collaboration), as well as the strengthening of regulatory and compliance frameworks, to ensure the secure deployment of these emerging technologies. Trust frameworks will also need to reflect societies' ethical and privacy values as digital security technologies advance.

[40] L. Williams et al. (2024) 'Uncovering Key Factors That Drive the Impressions of Online Emerging Technology Narratives', *Information*, 15, 706.

[41] L. Williams et al. (2025) 'The Evolution of Digital Security by Design Using Temporal Network Analysis', *Informatics*, 12, 8.

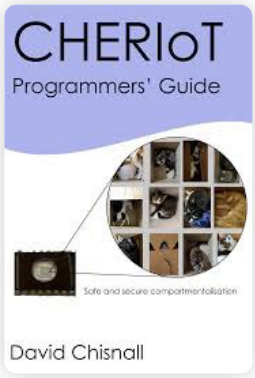
Futures, anticipation and **digital security**

Comedy, tragedy, quest or adventure; thriller or horror story: how do we imagine our digital future? Fraught with threat or sunlit uplands?

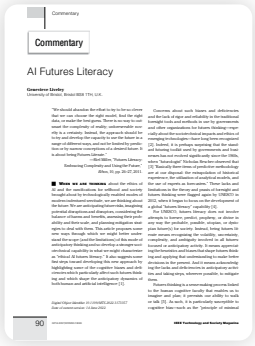


Discribe and the Jean Golding Institute invited creative writers worldwide to submit short stories to animate the secret life of data in a competition which attracted more than 200 submissions. Ten were chosen for the book, Secret Life of Data. They feature a palace protected by well-trained guards but vulnerable to human error, cat videos and couriers, precious memories and mythical landscapes. **The stories give research communities, policy makers and technologists new insights into some of our fears, hopes and dreams about the use of our digital data.**

> *'Analogy is how we imagine and make sense of new and complex concepts. And such creative imaginings... generate new insights into the possibilities involved in the adoption of new secure technologies in the context of a **volatile, uncertain, complex and ambiguous future**'*
>
> – Genevieve Liveley and Lizzie Coles-Kemp



Cats also feature on the cover of the draft CHERIoT Programmer's Guide, each in a separate, isolated, compartment. 'What could be more secure than a cat in a box?' asks author David Chisnall. Discribe funded the guide's development from work in progress to draft, now undertaking technical review. It will be published in HTML, PDF and printed formats, all including documentation plus examples and exercises (which were absent from earlier, incomplete versions). The guide gives developers a grounding in CHERI, the extra features of CHERIoT, and in designing compartmentalised software. It addresses needs identified in WP2 (page 12).



Liveley and Coles-Kemp emphasise the need for stakeholders to 'avoid simplifying or restricting the range of possible futures'. This means looking beyond the future as a continuation of the recent past and present (avoiding 'BAU' thinking) and interrogating binary distinctions between apparently utopian or dystopian futures. Scenarios with potential desirable (utopian) opportunities for one community may represent undesirable (dystopian) risks or compromises for others. Their work also revealed fragmented expectations among the DSbD community of:

- the possible, plausible, probable and preferred futures attending the next generation of security hardware technologies
- the value proposition of DSbD/CHERI

Such findings emphasise the value of 'futures literacy' – which extends to debates about the use and ethics of AI (Lively).

[42] G. Lively (2022) 'AI Futures Literacy', IEEE Technology and Society Magazine, June.

Forthcoming developments; **digital carrots and sticks**

The scale of the digital security challenge – and society-wide adoption of secure technologies and practices – can be daunting but adoption will drive innovation, build trust and enable growth, noted Rod Latham, Director for Cyber Security and Digital Identity, DSIT at the 2025 UK DSbD Showcase. Latham gave a clear signal of Government intent to continue to collaborate and support work to develop DSbD technology and drive adoption.

Forthcoming developments demonstrate the complexities innate to digital security by design, its adoption and regulation: multiple funders, investees, stakeholders, regulators, government departments, interlinking dependencies, overlapping missions:

- The Cyber Security and Resilience Bill, due to be introduced to Parliament in 2025, is likely to update and expand the scope of current Network and Information Systems Regulations and require organisations to increase their reporting of data breaches.
- Full adoption of operational resilience rules[43] that the Financial Conduct Authority requires firms in the financial services sector to adhere to (a 'transition period' ends on 31 March 2025).
- Potential updates to digital security guidance by other regulators.
- Potential updates to the five DSIT codes of practice on cyber security, including the Code of Practice for Software Vendors.
- The launch of more than 30 new skills projects (in England and Northern Ireland) to bolster UK cyber defence, funded by DSIT.[44]
- New Innovation and Knowledge Centres, funded by UKRI, to deliver new semiconductor technologies to market, alongside semiconductor skills projects across 32 organisations supported by Innovate UK, and other UKRI-funded work on Improving and Scaling-up Semiconductor Manufacturing. These projects support the government's national semiconductor strategy and seek to develop resilience, skills, and economic opportunity.

The right incentives at the right time

DSIT's own research[45] into CHERI adoption and diffusion found the **critical supply-side decision-making sectors for adoption to be chip designers and software development**. It identified **key demand sectors** for CHERI adoption, too, and called for more work to explore use cases and the economic benefits from adopting CHERI (emphasising the need to: craft messaging to highlight economic benefits; market CHERI as an investment with positive ROI, not an ongoing security cost; use real-world examples of security incidents that would have been prevented by CHERI; and work with companies that hold influence over software ecosystems to build awareness and share tools). It also identified **procurement as a potential enabler**, raised by Government stakeholders and at (Discribe-convened) DSbD 'all hands' events.

Discribe has complemented this research. An important lesson from our work is **how the extent, scope, reach and complexity of digital security requires collaboration, education and the right incentives, used at the right time.** Another is that **adoption isn't linear**: it is complicated and systems-based. Multiple elements determine whether a technology is adopted at scale. Whatever carrots and sticks are applied, trade-offs are inevitable.

[43] 'Operational resilience: insights and observations for firms'. Financial Conduct Authority (2024).

[44] 'New regional skills projects to bolster UK cyber defence and deliver Plan for Change' (2025). Department for Science, Innovation and Technology: Press release. Also 'List of Cyber Local projects', policy paper, 202.

[45] 'CHERI adoption and diffusion research' (2024). Department for Science, Innovation and Technology and Viscount Camrose.

Reflections, future challenges and the value of **technical alchemy**

Discribe's research demonstrates that social scientists add enormous value to technical and engineering projects. Technological solutions have and will continue to make the digital world more secure. However, technologies exist within evolving societies, and the adoption of digital security by design technologies will be a socio-technical one. Understanding DSbD within the context of an innovation system would help clarify the ways in which adoption can be more widely supported (e.g., by identifying the key functional elements needed such as niche markets). **Effective policies for socio-technical transitions must coordinate and convene multiple actors across various levels and institutions.**

It's easy to present roadmaps towards technology transitions or the adoption of new technologies. They can describe paths towards a vision, with a timeline and interrelated layers such as technology, markets, sectors and policies. But they can fail to address the shifting sands of wider socio-political and geopolitical landscapes. Processes and practices that had been taken for granted can suddenly be no longer applicable. The world has changed dramatically during the DSbD programme. Many recent developments make the case to 'fix the foundations' of the digital world stronger, while transition remains challenging. The post-pandemic world is increasingly characterised by national strategies emphasising technological sovereignty, a contrast to open-source practices of the 1990s and early 2000s.

With human behaviour and motivation at the centre of our thinking, **Discribe has identified 'can-do' gaps, asked challenging questions, uncovered unforeseen consequences, identified barriers and enablers to adoption, and built fruitful, collaborative relationships.** We have increased awareness and understanding of the barriers to digital security success and strengthened the ecosystem's ability to catalyse adoption – notably, not only the adoption of secure but design technology but of stronger, more secure organisation- and system-wide processes and practices.

Perhaps it makes more sense to create a river with multiple, alternative pathways through the shifting sands we live in than try to follow a rigid roadmap towards a secure future. We value the DSbD programme's flexibility, which enabled it to support spin-offs and emerging opportunities – and how, through Discribe, it combined social-science related skills such as reflexivity with technical skills.

Such technical alchemy addresses the 'cyber-GDP gap', adds significantly to our understanding of opportunities digital security offers across all parts of our society, and can contribute to goals such as technology leadership, maintaining the UK as a cyber power and world leader in digital security, and sustainable, inclusive economic growth.

[46] R. A. A. Hekkert et al. (2007) 'Functions of innovation systems: A new approach for analysing technological change', *Technological Forecasting and Social Change*, 74(4), pp. 413-432.

discribe

discribehub.org

Acknowledgements

The Discribe Hub+ would like to thank ESRC/UKRI for their support (grant reference: ES/V003666/1) and the wider DSbD programme and stakeholders for their engagement and support with the community building, futures work and research within Discribe.

UK Research and Innovation

University of Bath

University of Bristol

Cardiff University / Prifysgol Caerdydd

Royal Holloway University of London

Report edited and designed by **Research Retold** (2025)