Digital Trust

Unlocking the Next Wave of Growth in the Digital Economy

SGTECH
WHERE TECH MEETS

Digital Trust

Unlocking the Next Wave of Growth in the Digital Economy

Published by

SGTECH
WHERE TECH MEETS

Presenting Sponsors

aws

NetSfere
Enabling Communication.

Supporting Sponsors

intel.

Lenovo

Microsoft

Published in 2022 by SGTech
79 Ayer Rajah Crescent #02-03/04/05
Singapore 139955

research@sgtech.org.sg
www.sgtech.org.sg

© 2022 All rights reserved

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system, without the written permission of the copyright owner.

Table of Contents

Wong Wai Meng
Chair, SGTech

Digitalisation offers new approaches to trust. Competitors who do not see eye-to-eye can still transact efficiently because technologies such as privacy-enhancing technologies, distributed ledgers (also called shared ledgers), coupled with good governance in processes now enable these interactions even without parties knowing who they transact with.

1 Preface by SGTech

Wong Wai Meng

Chair, SGTech

Trust is defined as a firm belief in the reliability, truth, ability, or strength of someone or something, one in which confidence is placed. Trust has always been the linchpin of strong relationships, especially between individuals and businesses. Digital Trust is the same thing but applied to digital technology.

The whitepaper that you are reading now captures the core findings of SGTech's Digital Trust Landscape Study. Interviews with over 80 local, regional, and global industry leaders in their respective fields were conducted to map out the landscape for Digital Trust.

Why is Digital Trust critical now? With the increasing merging of the physical, digital, and biological worlds, it has created huge opportunities but also challenges for the way we live and work. The advent of technologies such as blockchain, artificial intelligence, big data, internet of things, and many more, has accelerated the pace of innovation in business. Internal resources alone are no longer sufficient for addressing the dynamic needs of markets; companies must adopt innovation strategies by collaborating with external stakeholders.

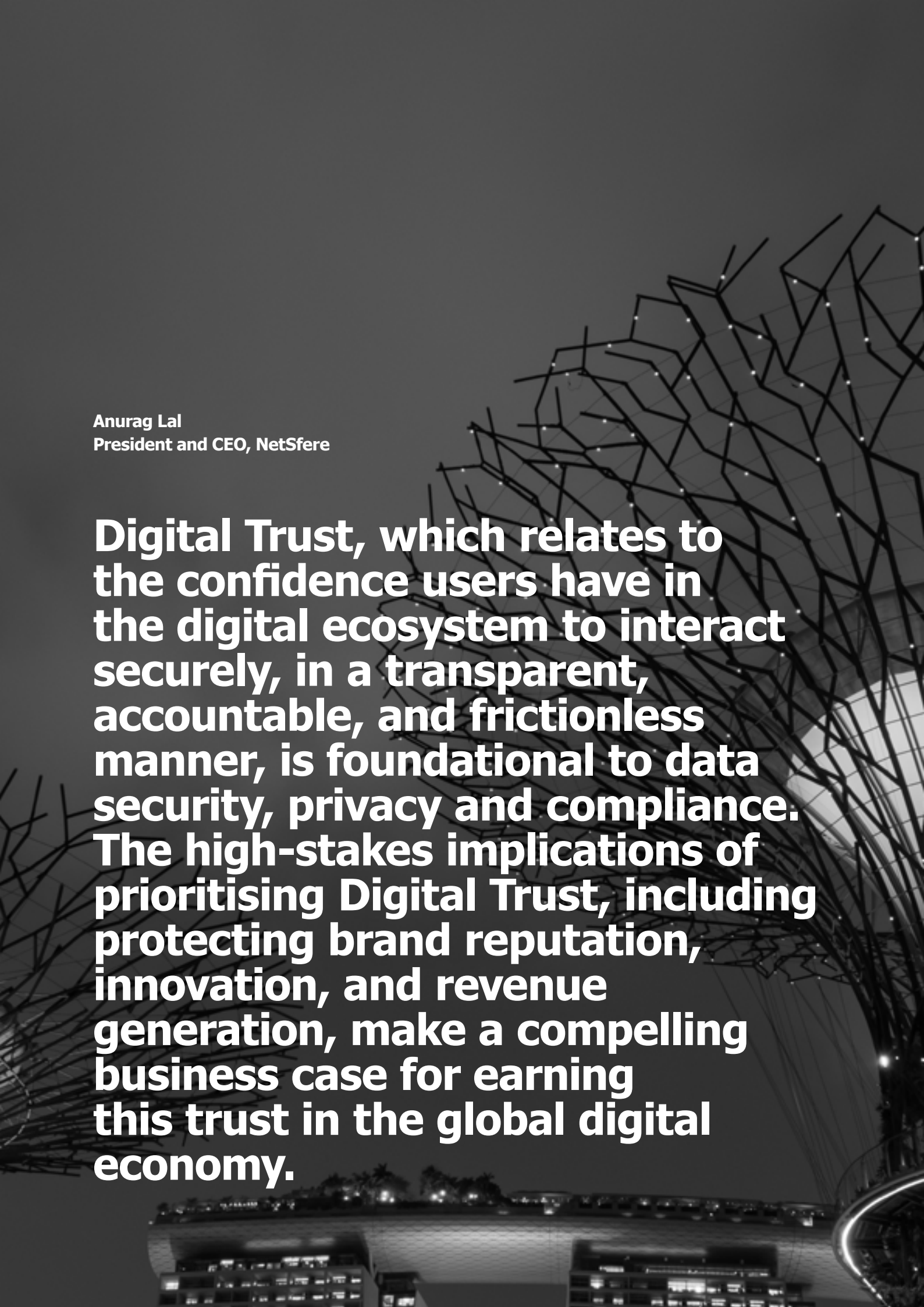
The push to digitalise and innovate has opened a can of challenges for companies, who must consider new privacy, security, and information-control issues as they collect and store more data. These concerns are exacerbated by increasingly polarised views on important topics, the spread of misinformation, and cybercrimes. SGTech believes that building digital and data systems based on trust is key to surmounting these challenges.

Our purpose in commissioning this study is to provide a global orientation of Digital Trust, its opportunities and challenges, and Singapore's importance as a global node for data and digital innovation. Digitalisation offers new approaches to trust. Competitors who do not see eye-to-eye can still transact efficiently because technologies such as privacy-enhancing technologies and distributed ledgers (also called shared ledgers), coupled with good governance in processes now enable these interactions even without parties knowing who they transact with.

Our study identified governance, technology, and people as three pillars that hold up the Digital Trust framework. Each pillar has enablers crucial to building a robust and trusted digital ecosystem. Cross-border cooperation, harmonisation of standards, and mutual recognition of certifications must continue to be encouraged. Education and capability-building of people will also be essential.

We hope this paper is helpful as a starting point to frame the subject. Beyond this whitepaper, more resources will be available at SGTech's Digital Trust Centre of Excellence. We invite you on this journey with us as we strengthen trust and further our common human pursuit of progress.

On behalf of SGTech, I would like to thank our members, industry partners, and the many contributors and interviewees who played a part in this Digital Trust Landscape Study. We are also grateful to the paper's presenting sponsors, AWS and NetSfere, as well as our supporting sponsors, Intel, Lenovo, and Microsoft.



Anurag Lal
President and CEO, NetSfere

Digital Trust, which relates to the confidence users have in the digital ecosystem to interact securely, in a transparent, accountable, and frictionless manner, is foundational to data security, privacy and compliance. The high-stakes implications of prioritising Digital Trust, including protecting brand reputation, innovation, and revenue generation, make a compelling business case for earning this trust in the global digital economy.

2 Foreword

Anurag Lal

President and CEO, NetSfere

This paper provides valuable insights and actionable strategies aimed at strengthening Singapore's digitalisation efforts and furthering Singapore's ambition to become a global node for Digital Trust. In the digital-first era, enterprises are increasingly communicating, collaborating, connecting, and transacting across channels. As the adoption of digital technology continues at a rapid pace, Digital Trust is elevated to a critical business enabler.

Digital Trust, which relates to the confidence users have in the digital ecosystem to interact securely, in a transparent, accountable, and frictionless manner, is foundational to data security, privacy and compliance. The high-stakes implications of prioritising Digital Trust, including protecting brand reputation, innovation, and revenue generation, make a compelling business case for earning this trust in the global digital economy.

Recognising the broad economic implications of earning Digital Trust, Singapore continues to invest in technological and skills initiatives to foster the growth of the Digital Trust ecosystem. In the thriving digital hub that is Singapore, opportunities abound for building digital services based on trust. And, as a leader in transparent governance, trusted regulatory frameworks and a respected centre of finance and law, Singapore is well-positioned to solidify its status as a leader in Digital Trust.

A key to establishing and advancing Digital Trust leadership involves working with security-first, privacy-first business partners that meet the operational imperative of earning and maintaining Digital Trust. This is especially critical in today's hybrid and remote working environments where more business than ever is conducted across digital channels.

A first line of defence for protecting Digital Trust is secure communication and collaboration technology, with end-to-end encryption and robust IT administrative controls. Enterprise-grade technology like this is a major strategic imperative for building Digital Trust, that ensures business continuity in a secure and compliant hybrid and remote working environment.

At NetSfere, we are partnering with Singapore-based companies in a wide range of sectors including financial services, healthcare, and government, to build a more trusted digital ecosystem and contribute to positioning Singapore as a global node for digital and data, built on trust.

We thank SGTech for commissioning this important report which maps out a strategic roadmap for developing Digital Trust in Singapore; all of the many contributors from around the world for providing their valued insights; and Eden Strategy Institute for compiling the insights and data into this whitepaper.

3 Executive Summary

Digital Trust is a SGD 385 bn (USD 270 bn) global market opportunity and is expected to grow to SGD 765 bn (USD 537 bn) by 2027. Digital Trust will also enable further growth in other sectors in the digital economy.

Trust has been a competitive edge for Singapore and led to its early success as a regional hub and attractive home for global businesses. An increasingly digital world amplifies opportunities for Singapore beyond the region, but only if Singapore can continue to be a trusted partner. With this lens, SGTech commissioned Eden Strategy Institute to study the Digital Trust landscape to help frame the topic and highlight the challenges and opportunities. This paper is a succinct summary of the broader landscape study conducted.

Between January and August 2022, an exhaustive review of existing Digital Trust literature and a series of over 80 interviews were conducted worldwide with leading experts in various Digital Trust domains. Through these insights, and extensive deliberations with SGTech's Digital Trust Committee and Council members, we have defined Digital Trust as follows:

> **Digital Trust is the confidence participants have in the digital ecosystem to interact securely, in a transparent, accountable, and frictionless manner.**

To achieve this, a range of enablers in Governance, People and Technology has been identified:

- **Governance:** Facilitate greater digital participation among good actors in an ethical manner, while putting in place mechanisms that resolve conflicts
  - AI Ethics Frameworks
  - Data Protection Laws and Regulations
  - Cyber Strategy and Laws
  - Cyber Insurance
  - Privacy by Design
  - Security by Design
  - Harmonisation Of Standards
  - Facilitating Bodies and Associations
  - Recourse and Mediation Bodies
- **People:** Develop discerning digital natives who can navigate the proper use of data and information, while keeping themselves and the organisations safe from bad actors
  - Consumer Awareness and Education
  - Citizen Advocacy
  - Digital Trust Certifications
  - Digital Trust Workforce
  - Digital Trust-Related Consultancy: Legal, Resilience Building, Training, Cybersecurity As-A-Service, Privacy-As-A-Service
- **Technology:** Overcome legal barriers while keeping in place the spirit of those laws, enhance online safety, and keep secure data and digital transactions from bad actors
  - Privacy Enhancing Technologies
  - Distributed Ledger Technologies
  - Cybersecurity Technologies
  - Digital Identity
  - Governance, Risk, and Compliance Software
  - AI/ML Tools: e.g., Fraud Detection, Threat Monitoring

Five key trends and opportunities were also identified in this study:

#1 Misinformation is becoming more widespread and affecting everyday people

- Consumer awareness and education to enable a more discerning population is essential

#2 Expectations on privacy and responsible use of data have grown and become mainstream

- The use of Privacy Enhancing Technologies (PET) could help adhere to the letter and spirit of the law, while generating the benefits that come from data sharing and analysis
- Embedding Privacy in products and services through Privacy by Design enhances transparency and accountability in an organisation's systems, and helps to increase confidence and loyalty in consumers and businesses they transact with

#3 Cybercrimes continue to grow unabated, especially in the Asia-Pacific

- Large companies will need to build up resilience capabilities, while Small and Medium Enterprises (SMEs), that are generally under-resourced, should consider cyber-as-a-service offerings
- Both large companies and SMEs should consider cyber insurance

#4 Data localisation, sovereignty and cross-border data flow issues are high on the agenda for many countries

- There is a strong need for data-sharing standards to be harmonised across countries, and there are opportunities to mutually recognise certificates that relate to Digital Trust; facilitation bodies such as APEC Business Advisory Council (ABAC) are important players that can drive these efforts
- Adoption of technologies, such as Digital Identity and permission-based Distributed Ledger Technologies, can also assist with more seamless and efficient cross-border interactions

#5 Growing demand for Digital Trust skills and risk management solutions

- A more sophisticated Digital Trust workforce will need new skills, as well as related services such as consultants, lawyers, training providers, and certification agencies
- Software solutions in Governance, Risk and Compliance (GRC) can also help companies better manage organisational risk and requirements for continuous compliance

There is no magic bullet to Digital Trust. Like trust in the physical world, Digital Trust takes time and effort to build up. The promise of Digital Trust is not just in the SGD 765 bn (USD 537 bn) industry that will be realised in 2027, it is the broader enablement of the digital economy and surmounting the trust challenges of today. These will result in a manifold multiplier in terms of more digital transactions and less losses from issues such as cybercrime. It offers new opportunities and a true differentiation to countries and companies that embrace it. We hope this paper helps you think more holistically about Digital Trust and provides pointers on where to start.

4 Introduction

Fostering trust in the digital world is increasingly vital in today's age of industry digitalisation, misinformation, and changing societal attitudes towards privacy.

There are many facets to the megatrend of Digital Trust. Digital Trust encompasses more than cybersecurity, privacy, data protection, or Artificial Intelligence (AI) ethics. At its core, creating Digital Trust demands no less than a concerted, full set of approaches that uphold stakeholder confidence and ensure that digital interactions truly work.

This paper aims to:

- Offer a broader definition of Digital Trust;
- Provide a global orientation on trust-related challenges in the digital arena;
- Provide a glimpse into the opportunities in Digital Trust; and
- Highlight Singapore's importance as a global digital and data node, built on trust.

Trust has always been foundational to Singapore's early success as a facilitator and partner for regional networks and global companies. A digital world opens Singapore up to wider global networks and opportunities. Its people, processes, and governance structures must be ready for the corresponding challenges, and Digital Trust is core to this readiness.

Singapore has been amongst the most progressive countries in Digital Trust:

- Recently opening a Digital Trust Centre focusing on trust technologies[1];
- Developing a Model AI Governance Framework and AI Body of Knowledge[2];
- Passing the Protection from Online Falsehoods and Manipulation Act (POFMA) in 2019[3];
- Implementing the Personal Data Protection Act (PDPA) in 2012, and rolling out Data Protection Officers (DPO) across its companies[4];
- Enabling Singpass, its national Digital Identity system, to be ubiquitous across government e-services and covering over 97 percent of eligible residents[5]; and
- Developing various Data Sharing Frameworks by the Infocom Media Development Authority (IMDA), Monetary Authority of Singapore (MAS)/Association of Banks in Singapore (ABS), and Singapore's Smart Nation and Digital Goverment Office (SNDGO)[6].

But more can always be done to unpack and frame the issues around the topic. This paper is the synthesis of a landscape study undertaken by the Digital Trust Committee of SGTech, Singapore's leading trade association for the tech industry, between January and August 2022. Eden Strategy Institute performed an exhaustive review of the global literature on Digital Trust and conducted a series of over 80 interviews across the world with leading experts in various Digital Trust domains.

5 What is Digital Trust?

From our expert interviews, review of existing Digital Trust literature[7], and deliberations with SGTech's Digital Trust Committee and Council members, this paper proposes a broader view of Digital Trust that extends beyond security.

Much of the existing Digital Trust literature has focused on cybersecurity and the components that secure digital systems and data flows. With legislative developments such as General Data Protection Regulation (GDPR) in Europe or PDPA in Singapore, the awareness of user privacy has been building up. In a trusted environment, there are opportunities to make digital transactions easier for everyone, allowing for individuals, businesses, and government participants to interact effortlessly across borders.

This paper therefore proposes the following definition of Digital Trust:

> **Digital Trust is the confidence participants have in the digital ecosystem to interact securely, in a transparent, accountable, and frictionless manner.**

This broad definition further finesses different emphases of Digital Trust for various stakeholders.

Citizens

Digital Trust is the confidence citizens have when they are interacting online, that their interactions are secure, remain private, transparent, and accountable.

Industry and Businesses

A business can inspire Digital Trust by being secure, competent, consistent, and transparent, and having a verifiable commitment to user interests, as demonstrated by its policies, systems, and conduct.

Governments and Regulators

Digital Trust is the adherence to necessary processes, policies, and frameworks around security, transparency, and accountability by the Government to enable businesses and consumers to interact efficiently and confidently in the digital world.

6 Challenges

To strengthen Digital Trust, it is useful to understand the challenges that will need to be addressed for the different stakeholders. There are a plethora of challenges but we present the most important challenges across our interviews.

Citizens

Misinformation

- Misinformation
- Disinformation
- Deepfakes driven by bad bots and foreign actors seeking to influence society

Online scams

Including:

- Hacking scams
- Phishing scams

Misuse of data

Where data analysis and personal information is used without consent

Online harms

Beyond misinformation, other forms of online harms such as:

- Child sexual exploitation and abuse content
- Cyberbullying
- Hate speech
- Online addiction
- Terrorism-related content
- Violent content

Misleading user interfaces

Where dark patterns and corporate interests misdirect consumers in their online interactions

Industry and Businesses

Constant cyber threats

Ensuring data and transmission are secure from external and internal intrusions, with necessary redundancy to recover from breaches

Online harms

Adhering to local and global regulations which are often disjointed and require local customisation; potentially high financial penalties for privacy regulatory failures

Inadequate capabilities

- Lack of baseline internal staff capability
- Hiring for specific skills such as cybersecurity and privacy engineers
- Retaining external support such as Digital Trust lawyers and Cybersecurity consultants

Lacking standards related to Digital Trust

Lack of standards that go beyond IT and cybersecurity, such as AI ethics frameworks, data sharing policies, or data classification

Constraints in data sharing

- Lack of trust between counterparties
- Data sovereignty and national laws restrictions
- Lack of available technology to manage Personal Identifiable Information (PII)

Under-resourced SMEs

Small and Medium Enterprises (SMEs) are especially vulnerable to cyber attacks, due to their lack of financial and manpower resources to put in place the necessary safeguards

Governments and Regulators

Facilitating data flows

Facilitating data flows, business cooperation within the country and across borders, while maintaining privacy concerns, cybersecurity, and national security

Complexities in cross-border cooperation

- Ensuring cross-border cybersecurity enforcement and sharing of intelligence on threats
- Cross-border data standards harmonisation through working with other governments and standard bodies

Foreign interference and disinformation

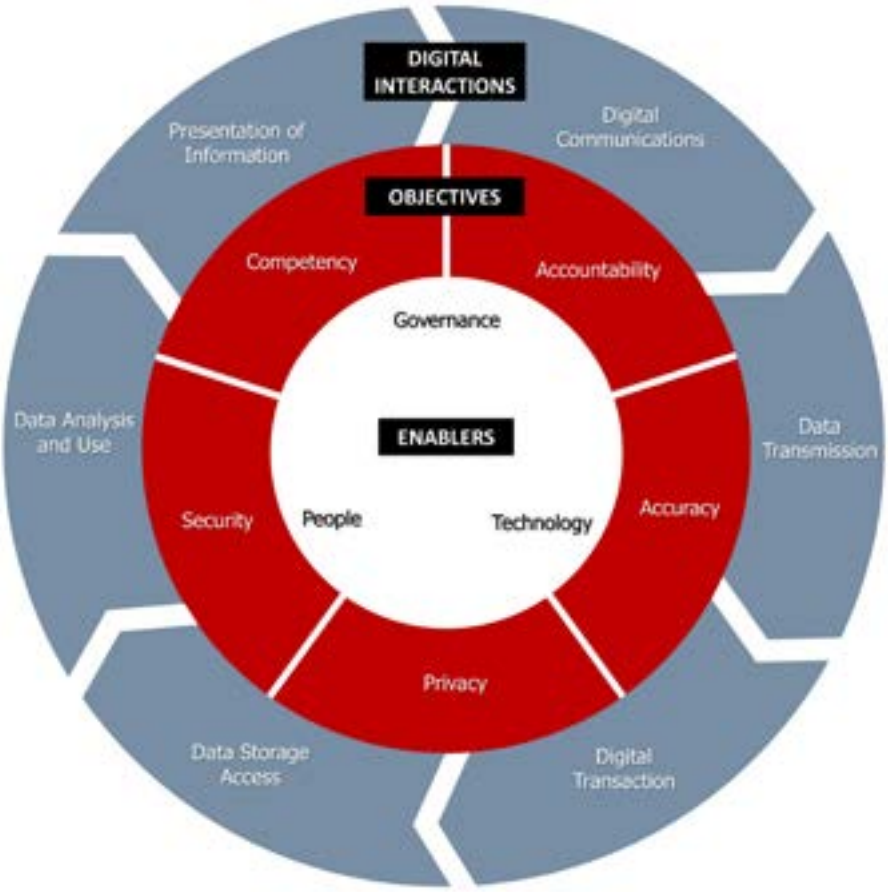
Educating the population and putting up defences to counter online threats

Global competition for talent

The global pull of Digital Trust-related talent such as in:

- AI ethicists
- Cybersecurity
- Digital Identity specialists
- Lawyers trained in international privacy regulations
- Privacy engineers

7 Enabling Digital Trust



Countries and organisations have a variety of options to holistically enable more trusted Digital Interactions.

There are five primary forms of Digital Interactions.

- **Presentation of Information:** e.g., Website viewing; hardware interfaces
- **Digital Communications:** e.g., Chats; video conferencing
- **Data Transmission and Digital Transaction:** e.g., IoT device transmissions; eCommerce transactions; B2B data transactions
- **Data Access and Storage:** e.g., Cloud storage; APIs; Digital IDs
- **Data Analysis and Use:** e.g., AI and Big Data analysis; wearables health monitoring; Know Your Customer (KYC)

The key objectives of Digital Trust in these interactions are:

- **Accuracy:** Information and data sources are accurate, timely, and comprehensive
- **Privacy:** Legal compliance and user confidentiality is respected
- **Security:** Data and transaction integrity is maintained and available only to the intended parties
- **Competency:** Digital Interactions are available and done efficiently and successfully
- **Accountability:** Use of the data or purpose of the use meets expectations and is done in a legal, ethical, and transparent way; failures such as data breaches or misuse of data are addressed quickly and responsibly

To enable these objectives, three sets of Enablers in Governance, Technology, and People are required:

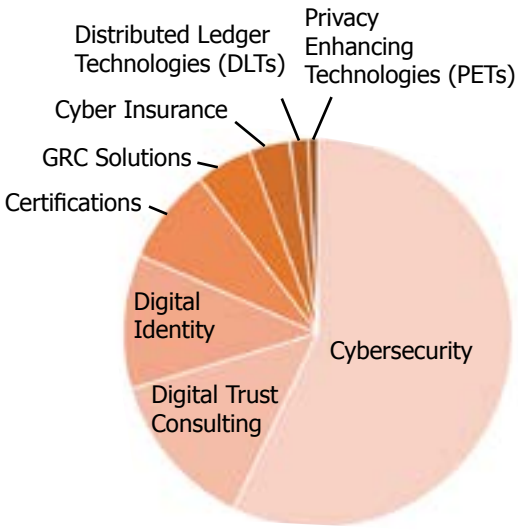
- **Governance:** Facilitate greater digital participation among good actors in an ethical manner while putting in place mechanisms that resolve conflicts
  - AI Ethics Frameworks
  - Data Protection Laws and Regulations
  - Cyber Strategy and Laws
  - Cyber Insurance
  - Privacy by Design
  - Security by Design
  - Harmonisation Of Standards
  - Facilitating Bodies and Associations
  - Recourse And Mediation Bodies

- **People:** Develop discerning digital natives who can navigate the proper use of data and information, while keeping themselves and the organisations safe from bad actors
  - Consumer Awareness and Education
  - Citizen Advocacy
  - Digital Trust Certifications
  - Digital Trust Workforce
  - Digital Trust-Related Consultancy: Legal, Resilience Building, Training, Cybersecurity As-A-Service, Privacy-As-A-Service

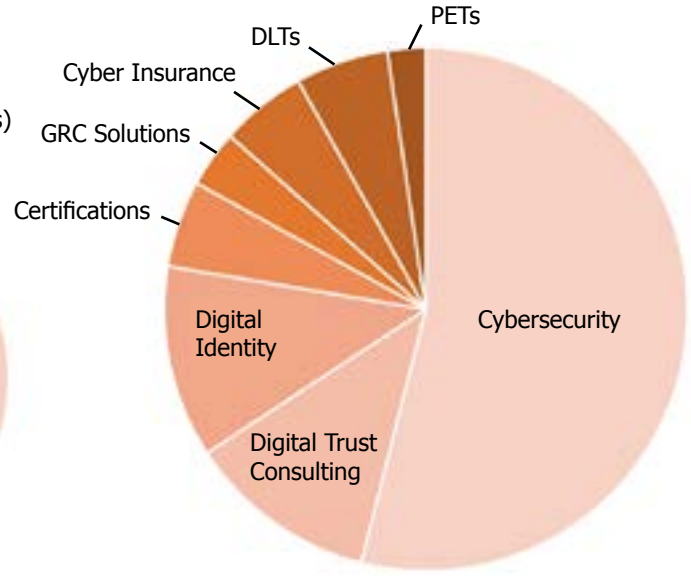
- **Technology:** Overcome legal barriers while keeping in place the spirit of those laws, enhance online safety, and keep secure data and digital transactions from bad actors
  - Privacy Enhancing Technologies
  - Distributed Ledger Technologies
  - Cybersecurity Technologies
  - Digital Identity
  - Governance, Risk, and Compliance Software
  - AI/ML Tools: Fraud Detection, Threat Monitoring, Synthetic Data, etc.

8 Sizing the Market for Digital Trust

Digital Trust presents a global market opportunity of SGD 385 bn (USD 270 bn) currently and is expected to grow to SGD 765 bn (USD 537 bn) by 2027.



Global Revenues by Digital Trust Enabler (SGD bn; 2022)



Global Revenues by Digital Trust Enabler (SGD bn; 2027 Estimates)

SGD bn

Headline	2022	2027	CAGR
Cybersecurity	220	415	13%
Digital Trust Consulting	51	90	12%
Digital Identity	43	91	16%
Certifications	31	41	6%
GRC Solutions	18	27	8%
Cyber Insurance	13	41	25%
Distributed Ledger Technologies (DLTs)	6	44	49%
Privacy Enhancing Technologies (PETs)	3	18	40%
Industry Total	**385**	**765**	**15%**

Source: Eden Strategy Institute Interviews and Analysis; Globe Newswire; Statista; Fortune Business Insights; Consultancy.org, IDC; Report Linker

Based on our research, interviews, and analysis, the global market for Digital Trust is growing at a Compounded Annual Growth Rate (CAGR) of 15 percent, and is expected to double to SGD 765 bn (USD 537 bn) over the next five years.

The size of the Digital Trust sector in Singapore currently stands at SGD 1.7 bn (USD 1.2 bn) (yearly revenue) with more than half of this coming from Cybersecurity. The sector also currently employs around 15,000 people and could grow to SGD 4.8 bn (USD 3.4 bn) (yearly revenue) and employ 34,000 to 45,000 people by 2027.

Cybersecurity, the most mature and largest segment, will continue to contribute most significantly in absolute terms. Digital Identity is also a relatively mature technology, with adoption continuing to pick up, as more countries look towards national digital transformation plans. For example, India has shown admirable success in creating the world's largest biometric Digital ID system, with its Aadhaar program enrolling 1.3 bn citizens (or 99 percent of Indian adults)[8]. The European Commission proposed a digital ID scheme in 2021, that could be used across the EU by more than 80 percent of the EU population by 2030[9]. China's Prime Minister Li Keqiang has recently announced that Digital IDs, which have been tested in China since 2018, will be rolled out nationwide in 2022[10]. Cross-border economic opportunities are also expected to be amplified, should these national Digital IDs become harmonised or interoperable regionally.

The market for emerging Digital Trust Technologies such as Privacy Enhancing Technologies (PETs) and Distributed Ledger Technologies (DLTs) is attracting venture capital interest, and companies are working to validate use cases for different types of data in various industries. Their potential to leapfrog regulatory requirements and scale trust in their systems makes them exciting hotspots for growth.

Cyber Insurance is gaining greater adoption from large companies, and is also expected to see an uptick from more widespread SME adoption.

Insurance companies are actively courting SMEs to help diversify their own risk portfolios.

Consulting, Certifications, and GRC Solution providers are capability-building sectors that tend to be early adopters, which will help accelerate Digital Capabilities across different industries and improve risk management practices.

SGD 765 bn

Global market for Digital Trust in 2027 (USD 537 bn), doubling from SGD 385 bn (USD 270 bn) in 2022

SGD 4.8 bn

Size of Singapore's Digital Trust Sector in 2027

34 - 45k

Size of Singapore's Digital Trust workforce in 2027

9 Global Trends and Opportunities in Digital Trust

Distrust is now society's default emotion, with six in ten people inclining to distrust until they see evidence to suggest that something is trustworthy.[11]

Seven percent more people in 2022, compared to 2021, believe that business leaders are purposely trying to mislead through false or exaggerated information. Mistrust towards media and government leaders is also proliferating, growing at a higher rate of eight and nine percent respectively.[12]

Covid-19 has accelerated digitalisation and teleworking, but it has also brought several challenges to the fore. Trust in technology companies in 2021 dipped to an all-time low, as the world grappled with increased cyber-attacks, data breaches, and 'bad bots' driving misinformation. Governments were not spared either; for example, democracies such as Australia, Germany, the Netherlands, South Korea, and the US saw the greatest declines in trust in 2022.[13]

Now, more than ever, governments and companies need to pay attention to Digital Trust. Based on our research and interviews with experts from domains of Digital Trust, the following five issues present the greatest challenges in Digital Trust to countries and organisations and need to be addressed.

#1 Misinformation is becoming more widespread and affecting everyday people

Fake news and misinformation driven by bots; fake unauthenticated accounts; "online trolls"; and foreign nation-state actors, are all eroding Digital Trust among consumers and citizens globally. It is becoming increasingly complex to distinguish between semi-true information and complete misinformation, and technology has not developed enough nuance to tackle this issue in a scalable and consistent way.

Singapore is ranked second among countries whose Internet traffic has high bad bot activity, according to a study across 192 countries. 39 percent of Internet traffic in Singapore was from bad bots, used to conduct malicious attacks, compared to 53 percent from people and eight percent from good bots.[14]

In a global survey across 25 economies, 86 percent of online respondents globally believe they have been exposed to fake news. Of these, over 85 percent reported that they initially believed it[15]. Although in Singapore most citizens do not deliberately spread fake news, they are exposed to misinformation by accessing global social media platforms and as many as 75 percent have unwittingly forwarded such information onto their personal networks.[16]

86%

Proportion of online respondents that believe they have been exposed to fake news[17]

39%

Bad bots as a proportion of Internet traffic in Singapore[18]

OPPORTUNITIES

Consumer Awareness and Education

More governments will act defensively and enact laws related to misinformation. For example, Singapore has passed the Protection from Online Falsehoods and Manipulation Act (POFMA), which seeks to counteract false or misleading information online[19]. This law covers public as well as closed platforms such as chat groups and social media groups.

Our interviews have indicated that social media companies are presently concerned about this issue, are taking decisive actions themselves, such as hiring large global teams to police content, deploying AI-based technologies to identify fake accounts, and limiting the spread of misinformation.

Governmental oversight and social media self-policing is necessary but not sufficient. There is a need to develop a more discerning population. **Greater consumer awareness and education** will be vital to manage the spread of misinformation, which presents an opportunity for governments, educational institutions, think-tanks, non-profits, and advocacy groups. School curricula and community awareness programs, particularly for the elderly, will also be necessary to improve consumer online savvy.

#2 Expectations on privacy and responsible use of data have grown and become mainstream

There has been a renewed demand for privacy, as a result of the missteps of social media giants and misuse of Big Data, such as in the Cambridge Analytica data scandal where personal data of users was collected and used without consent for targeted political advertising[20]. The growing awareness of data bias and opaque decision-making in AI, which in some high-profile cases has resulted in racial profiling[21], has also prompted caution and unease in the use of AI.

Globally, 80 percent of countries have some sort of data privacy regulation or draft data privacy regulation[22]. Europe has traditionally been the dominant force in privacy regulation with the EU General Data Protection Regulation (GDPR), for which Germany and France are key anchor nations[23]. The proliferation of data regulations has accelerated, with Asia, Africa, and South America coming on board with their own data protection laws.

However, this number is only 69 percent for Asia-Pacific Countries[23]. More developed privacy regime standards are expected to take form, with more countries following the stringent standards found in EU GDPR, such as provisions on extra-territorial reach and data transfer.

Many ASEAN countries have based their privacy regulations on the GDPR, although privacy regulations are at different stages of development. Many governments in the region are still educating themselves on data privacy approaches that would be appropriate to their contexts, and have yet to institutionalise new regulations.

Chinese tech companies are ramping up their privacy protections to meet the expectations of the national government and Chinese people, to be more transparent, secure, and accountable, as well as to fully comply with the recently passed Personal Information Protection Law (PIPL)[24].

The US does not have a comprehensive federal level data privacy law, although one is currently being negotiated. Nonetheless, there is a growing number of states that have adopted their own data protection laws, such as the California Consumer Privacy Act (CCPA) which came into effect in January 2020, and the California Privacy Rights Act (CPRA) which comes into effect in January 2023[25].

Singapore has an AI framework to guide companies on ethical AI use[26], without legislating specific AI laws so far. Countries such as the UK, US, and Spain passed AI-related legislation in 2021. The EU is now working on an EU AI Act, which could influence other countries' AI standards, akin to how the EU GDPR has influenced many countries' privacy policies. More than 60 countries have adopted some form of AI policy[27], as the world ramps up the pace of AI adoption.

69%

Proportion of Asia-Pacific Countries that have data privacy regulation or draft data privacy regulation[28]

OPPORTUNITIES

- **Privacy Enhancing Technologies (PETs)**
- **Privacy by Design**

Increasing privacy governance requirements are at odds with the increasing ways data is used, such as with Artificial Intelligence / Machine Learning (AI/ ML) models. **PETs** are a collection of methods to do encrypted computation on sensitive or protected data, such as Personal Identifiable Information. PETs can satisfy data-sharing constraints imposed by privacy regulations.

They can also help hide sensitive non-private data, such as telco tower geolocations, fleet routes, or eCommerce buying patterns. These technologies promise a future where datasets will no longer need to be exchanged, for cross-dataset machine learning benefits to be reaped.

PETs will unlock more AI/ML use cases and advance new insights. We see a future where datasets are made voluntarily available across different industries; there are already green shoots of consortiums such the Melloddy Project – a group of pharmaceutical companies including GSK, Bayer, and Merck – collaborating on drug discovery because richer datasets have been made available. Regulations around AI use will be even more critical in this supercharged environment. Countries and companies will need to have in place their own AI frameworks as well as governance policies.

But privacy regulations and PETs are only part of the solution. The default posture of companies should be to provide privacy assurance across their products and services, embedded into the design and architecture of IT and business practices.

Interviewees reported increases in revenue and customer loyalty, with consumers feeling safer and more confident to interact with companies that they feel are accountable and transparent in how they use their data. To achieve this, organisations can consider adopting the principles of the **Privacy by Design** Framework, developed by former Ontario Privacy Commissioner Ann Cavoukain, which outlines seven foundational principles[29].

#3 Cybercrimes continue to grow unabated, especially in the Asia-Pacific

There has been a rise in cyber-related crime globally. Worldwide cybercrime cost USD 6 trn in 2021, growing at 15 percent Y-o-Y reaching USD 10.5 trillion by 2025[30]. Ransomware is the fastest-growing cybercrime, with damages in 2021 estimated at USD 20 bn - 57 times more than it was in 2015[31]. Ransomware repercussions can be significant. In May 2021, the Colonial Pipeline fuel company in the US was forced to pay USD 5 mn in ransom, and the attack caused major gas shortages in the southeast coast of the US[32].

The growth in cyberattacks in Asia-Pacific is perhaps more serious than the global average, with a 168 percent increase between May 2020 and May 2021 alone[33]. Dark net-related arrests in Southeast Asia have increased in recent years, indicating that criminals perceive the region as a low-risk/high-gain operational environment, where the likelihood of detection remains relatively low.

The region is plagued with enforcement and coordination problems. Regional threat assessment sharing and mapping of cybercrime are missing. Crimes are often cross-border, making enforcement difficult. Penalties also do not seem proportionate to the harm done, and cyber criminals around the region understand how to work the system to reduce their culpability.

Regional players see Singapore as serious about cybersecurity. Singapore has a dedicated Cybersecurity Act, a clear Cybersecurity Strategy developed in 2021, and a vibrant cybersecurity ecosystem underpinned by a strong Cybersecurity Agency. Nonetheless, it is a target as it has a big financial sector, and is one of the most connected nations in the world. Singapore is constantly under threat, with cybercrime comprising 48 percent of all crime in the country.[34]

Cybercrime Statistics

Global	US	Asia-Pacific	Singapore
USD 6 trn	**300%**	**168%**	**38%**
Cost of Cybercrimes in 2021[35]	Increase in Cybercrimes reported by the FBI since the pandemic[36]	Increase in Cyberattacks between May 2020 and May 2021[37]	Growth of Cybercrime cases between 2020 and 2021[38]

OPPORTUNITIES

- **Resilience Building in Large Enterprises**
- **Cybersecurity as-a-Service for SMEs**
- **Cyber Insurance**

Large enterprises and governments will constantly play a game of cat and mouse with cyber criminals. Cybersecurity products also tend to be costly and catered more towards large enterprises. Beyond shoring up on products and talent, sophisticated **large enterprises will build up resilience capabilities** and be able to respond and recover from cyber-attacks. Large companies should line up their public relations, legal, and forensic consultants before an incident happens, as there is little time to react by the time a breach occurs.

Governments and large enterprises can look at roadmaps and frameworks such as Singapore's Cyber Security Agency Cyber Trust Certification's Five Tiers[39] to understand how they can advance in the journey.

Most vulnerable are SMEs who lack resources and awareness about improving cyber hygiene. Many small companies are at a loss on where to start. SMEs are unlikely to add headcount for cybersecurity and should consider **Cybersecurity as-a-Service** (ie. outsource their cybersecurity needs) from third-party companies. However, these services will have to be priced low to serve this price-sensitive market, and even subsidised by the government as a public good.

Cyber Insurance is an interesting area which can spur cyber hygiene, as getting it requires companies to adopt a certain standard of corporate cyber-readiness. We estimate the demand for Cyber Insurance to be growing at 25 percent Y-o-Y. There is an increased interest from insurance companies to expand their offerings to SMEs to diversify their portfolios. By using Cyber Insurance, companies can protect against losses stemming from data destruction, theft, extortion, hacking, and network intrusion or interruption. Increased awareness and adoption of Cyber Insurance should be considered by all large companies and even most SMEs.

25%

Annual Cyber Insurance market growth

#4 Data localisation, sovereignty, and cross-border data flow issues are high on the agenda for many nations

62

Countries that have enacted data localisation requirements[40]

The importance of localisation and sovereignty has risen over the years due to privacy concerns, cybersecurity, and national security. More than 62 countries have enacted data localisation requirements in 2021, up from 35 in 2017. The number of related policies has also doubled from 67 to 144 in the same period[41]. For example, China requires data localisation for the broadly-defined Critical Information Infrastructure operators. Transferring data outside of China involves security assessments conducted by the Cyberspace Administration of China (CAC)[42].

Pivotal events such as the Edward Snowden National Security Agency (NSA) data collection revelations[43], as well as the enactment of the US Patriot Act[44] - which allows the US government to access information from US-based servers - have further heightened national data sovereignty concerns around the world. Nonetheless, the US is one of the strongest opponents to data localisation restrictions; there are no special requirements to transfer personal data from the US to third-party countries.

The EU is more restrictive but does not require certain personal information to remain in the EU. Cross-border data transfers to third-party countries, however do need to respect GDPR either through being countries on the EU "Adequacy Decision" list, or applying appropriate safeguards such as Standard Contractual Clauses (SCCs). It should be noted that only 14 countries are on the Adequacy Decision list, with no ASEAN representation. 94 percent of global data transfers are based on Standard Contractual Clauses[45].

These policies make cross-border data flows difficult. Complying with cross-border data transfer laws is cited as the most difficult task for privacy professionals[46].

To address this, ASEAN is trying to move together on data protection and data flows. For example, ASEAN has already implemented Model Contract Clauses for cross-border data flows[47]. These are important steps in coordinating data regulatory policies. Strategic priorities for the ASEAN Digital Data Governance Framework include data flow mechanisms with particular focus on certification as well as regulatory sandboxes. The Philippines and Singapore are like-minded partners driving this trend, and are instrumental in the adoption of the ASEAN Digital Data Governance Framework.

OPPORTUNITIES

- **Harmonisation of Standards**
- **Facilitating Bodies and Associations**
- **Digital Trust Certifications**
- **Cross-border Digital Identity**
- **Permission-based Distributed Ledger Technologies (DLTs)**

Associations and harmonised standards will play increasingly important roles to facilitate data sharing. Various initiatives such as the APEC Cross-border Privacy Rules (CBPR) and Global CBPR Forum seeks to help companies share data through common standards and mutual recognition of certificates[48]. SGTech and the APEC Business Advisory Council (ABAC) have entered into a partnership to further the APEC CBPR agenda as well as develop a Digital Trust Centre of Excellence to promote greater multi-lateral trust mark integration and recognition. These efforts will take time to develop momentum, and will benefit from greater participation among both countries and companies globally.

As more countries create Digital Trust-related policies, more companies will adopt various **Digital Trust certifications** as a source of validation and prove their trustworthiness. APEC CBPR is one such certification for data sharing, and others include the ISO 27001 on information security, CSA Cyber Essentials and Cyber Trust marks for cybersecurity, and GDPR and PDPA practitioner certifications for personal data protection that touch on the other aspects of Digital Trust.

Trust-related technologies such as **Digital Identity, Distributed Ledger Technologies (DLTs)**, and PETs can also help play a role in improving data flows. Digital Identity helps verify the authenticity of information, be it from a company, individual, or IoT device. Opportunities for cross-border collaboration on Digital Identity will help to reduce frictions in data flow and data access, and could even spur greater cross-border digital transactions. Companies such as Mastercard[49] are seeking to help orchestrate these cross-border Digital Identity collaborations, developing technology, liability, assurance, and commercial frameworks to enable this.

The resilience, transparency, and accountability found in DLTs has garnered strong interest from regulated industries, especially within the financial services sector, through "Private" blockchains where participants are validated before being accepted. The Monetary Authority of Singapore (MAS) has undertaken a series of experiments looking at several use cases for DLTs, such as tokenisation of the SGD, local and cross-border inter-bank payments and settlements, and Central Bank Digital Currency (CBDC). It actively involves the private sector and other central banks in these collaborations. For example, its most recent initiative, Project Dunbar[50], is a collaboration between MAS, the BIS Innovation Hub Singapore Centre, the Reserve Bank of Australia, Bank Negara Malaysia, and the South African Reserve Bank.

Even though ASEAN countries are still in the early phase of DLT adoption, blockchains already feature in all ASEAN Member's ICT Master Plans[51]. DLT's consensus mechanisms enable data and its processing to be resilient from attacks, allowing control to be held in the hands of the registered participants themselves. There is no need to either trust the counterparty or rely on an intermediary to process, as the transaction is verified by the system's specified governance protocol.

#5 Growing demand for Digital Trust skills and risk management solutions

Government regulations and data protection fines are on boardroom agendas, as they now pose existential risks for companies. In Singapore, the maximum financial penalty that may be imposed on organisations for PDPA breaches has now increased from the previous maximum of SGD 1 mn, to SGD 1 mn or 10 percent of the organisation's annual turnover, whichever is higher[52]. Similarly, companies with EU exposure can be fined up to EUR 20 mn or four percent of worldwide turnover (whichever is greater) for GDPR breaches[53].

This has created a demand for new specialised Digital Trust skills such as privacy engineers and Data Protection Officers (DPO). These roles are increasingly important to large organisations that deal with large amounts of data, such as large consumer tech companies. Small companies in Singapore are also required to designate at least one individual to act as a DPO. There is also a war on talent for "traditional" cybersecurity professionals. The number of unfilled cybersecurity positions globally is growing from one million in 2013, to an estimated 3.5 million in 2025[54].

Large companies are also beginning to invest in general Digital Trust education for their employees. These begin with cybersecurity hygiene matters, and can often extend to organisation risk management.

3.5 mn

Estimated number of unfilled cybersecurity positions in 2025[54]

OPPORTUNITIES

- **Digital Trust workforce and skills**
- **Digital Trust Service providers**
- **Adoption of GRC technologies by companies**

A more sophisticated **Digital Trust workforce** and providers of **Digital Trust-related services**, such as consultants, lawyers, and training providers are becoming more prevalent. Digital Trust practitioners will graduate with Degree and Diploma courses in highly-specialised domains. Cutting-edge companies are also looking for multi-disciplinary talent who can bridge the divide between policy, compliance, AI ethics, and technology. In the future, more global companies will form small multi-disciplinary teams with a global Digital Trust mandate, creating strong competition for such talent globally.

Organisations will also look to imbue their entire workforce with Digital Trust-related training. Companies will increasingly invest in continuous compliance and real-time risk assessment. More and more organisations will opt for **Governance, Risk, and Compliance (GRC)** solutions to help them manage this undertaking, where inputs from everyday employees will flow into GRC systems to provide a more macro view of organisational risk. GRC software is already seeing a 20-30 percent increase in interest in Singapore[55] and an eight to 14 percent growth rate globally[56].

10 Concluding Remarks

Royce Wee
SGTech Digital Trust
Exco member &
Lead for Digital Trust
Landscape Study

Digitalisation is one of the key trends of our times. For digitalisation to fulfil its promise, we need to put Digital Trust front and centre of our efforts to develop and regulate the digital economy.

The Digital Trust Landscape Study, as summarised in this paper, represents an essential effort by SGTech and the tech industry to understand and unpack this large, complex, cross-border, and multi-faceted topic through research, interviews, and analysis with experts, government leaders, and captains of industry from around the world.

Having put a solid conceptual framework on what Digital Trust is, its enablers, and its challenges, the Digital Trust Landscape Study is very much at the beginning of its important work.

This is because the study, perhaps more crucially, also represents a clarion call to action for all the essential stakeholders in the digital ecosystem.

First, our laws, policies, and regulations have to be appropriate, balanced, and fit-for-purpose to secure and facilitate Digital Trust. This will ensure that digital technologies continue to be at the service of humans, and enable tech development to be on a healthy and sustainable track.

Second, corporations will do well in viewing the incorporation and demonstration of Digital Trust as a key competitive differentiator and advantage. Where corporations display Privacy by Design and Security by Design, adopt privacy-enhancing technologies and governance, risk and compliance tools, invest in their cybersecurity, and have third-party certifications to review and validate their systems and processes, they are much better-placed to win and retain their customers, as well as innovate using the data they have to come up with new products and services in a responsible and trusted manner.

Third, employees and customers also have much to look forward to. Employees will be able to access new training and upskilling courses to master new Digital Trust capabilities, for instance, across data protection, cybersecurity, fair market conduct, and ethics. Customers will be entitled to greater transparency in the data processing activities of corporations, have more agency and choice over the granting of access to their data, and be able to exercise their data subject rights more easily.

As technology doesn't stand still, there will be a recurring need for Digital Trust to continue to evolve. For example, as Web 3.0 takes shape, marked by greater decentralisation, digital assets, and AR/VR experiences, future research will have to be done across the technology, governance, and people pillars to see how digital trust can take root in and propagate across the Web 3.0 digital ecosystem.

We are on the cusp of great and accelerating change driven by rapid tech changes. By securing Digital Trust through a close and collaborative partnership across the public, private, and people sectors, all of us can have the confidence and optimism to ride the wave of change successfully.

In this regard, SGTech has been having early conversations on Digital Trust which are now becoming regional and global conversations and projects. I urge you to get in touch with SGTech if you would like to learn more, and prepare your organisation to build its capabilities and join our growing Digital Trust ecosystem.

“We are on the cusp of great and accelerating change driven by rapid tech changes. By securing Digital Trust through a close and collaborative partnership across the public, private, and people sectors, all of us can have the confidence and optimism to ride the wave of change successfully.

11 Acknowledgements

The SGTech Digital Trust Committee wishes to acknowledge and thank the numerous contributors who provided their valuable insights that informed this study.

SGTech Digital Trust Committee Patron

Mr Tan Kiat How	Senior Minister of State, Ministry of Communications and Information & Ministry of National Development

SGTech Council Chair

Mr Wong Wai Meng	Chief Executive Officer, Keppel Data Centres

SGTech Council Members

Mr Dutch Ng	Co-Founder & Chief Executive Officer, i-Sprint Innovations
Mr Gavin Chua	Head of Stakeholder Engagement, APAC, Meta Singapore
Mr Ivan Chang Weilong	Consumer Payments, Walt Disney Company
Mr Michael Yap	Co-Founder & Managing Partner, TNB Ventures
Ms Jessie Jie Xia	Global Chief Information Officer, Thoughtworks

SGTech Digital Trust Council

Mr Chun Li	Chief Executive Officer, Lazada Group
Mr Ishan Palit	Member, Board of Management, TÜV SÜD AG
Mr Tham Sai Choy	Independent Board Director, DBS Bank

SGTech Digital Trust Committee Members and Study Advisors

Mr Philip Heah	Chief Executive Officer, Credence Lab & Digital Trust Committee Chairman
Mr Royce Wee	Director, Head of Global Public Policy, Alibaba & Digital Trust Landscape Study Lead
Dr Bhaskar Chakravorti	Dean, Global Business, The Fletcher School, Tufts Univ & Landscape Study Special Advisor
Dr Katharina Von Knop	Founder & CEO, Digital Trust Analytics & Landscape Study Special Advisor
Mr Calvin Chu	Managing Partner, Eden Strategy Institute
Mr Chester Chua	Head of Google Cloud, Government Affairs & Public Policy, Google
Mr David Alfred	Director and Co-Head, Data Protection, Privacy & Cybersecurity Practice, Drew & Napier
Ms Jene Lim	Head of Product Management, Experian Asia Pacific
Mr Raju Chellam	Vice President New Technologies, Fusionex
Mr Satya Ramamurthy	Partner, Head of Infrastructure, Government & Healthcare, Head of Strategy, Advisory, Global Co-Head of Public Transport, KMPG
Ms Sowmya Krishnan	Head of Data & AI, SEA, ThoughtWorks
Ms Thao Dang	Head of Enterprise Modernisation, Platforms and Cloud, ThoughtWorks
Mr William Anstee	Chief Executive Officer, Totally Awesome

Expert Interviewees

Dr Adam Chee	Chief, Smart Health Leadership Centre, Institute of Systems Science, National University of Singapore
Mr Adam Wojtonis	Founder & Chief Executive Officer, MonkPhish
Ms Aileen Chew	Area Country Manager, Mastercard Thailand & Myanmar
Mr Alan Chan	Chief Risk Officer, Lazada Group
Mr Alexandru Caciuloiu	Cybercrime, and Cryptocurrency Programme Coordinator, UN Office on Drugs and Crime (UNODC)
Mr Alister Leong	Vice President - Product, SOL-X
Mr Alvin Toh	Chief Marketing Officer, Straits Interactive
Mr Andre Shori	Chief Information Security Officer for the Asia Pacific Region, Schneider Electric
Dr Andreas Hauser	CEO Digital Service, TÜV SÜD
Mr Ankur Gupta	Senior Vice President – Asia Regional Team, Marsh
Dr Ann Cavoukian	Founder and CEO of Global Privacy and Security by Design
Dr Arianne Jimmenez	Privacy and Public Policy Manager, APAC at Meta
Mr Bastian Purrer	Co-founder, HumanID
Mr Bruce Liang	Head of Strategic Projects, SEA Group
Mr Cai Yilun	Head of Presales & Solutions (SEA) SenseTime
Mr Charles Ng	Executive Vice President, Ensign InfoSecurity
Mr Charles Radclyffe	CEO, EthicsGrade
Ms Chatrini Weeratunge	Global Risk Ops, Trust & Safety, Meta
Dr Chi Hung Chi	Director, the Strategic Centre for Research in Privacy-Preserving Technologies and Systems (SCRiPTS), NTU
Mr Chng Kai Fong	2nd Permanent Secretary, Smart Nation and Digital Government Office (Singapore)
Mr Clement Teo	Senior Vice President, Business Assurance (ASEAN) at TÜV SÜD
Mr David Tan	Senior Vice President, Political Risk & Structured Credit ASEAN Sales Leader, Marsh
Mr Deb Pal	Director, Digital Trust/Cyber Security, PwC
Mr Devesh Narayanan	Researcher in AI ethics
Mr Dominic Chan	Director, National Digital Identity, GovTech Singapore
Ms Elizabeth Chee	Head of Govt. & Enterprise Sales, Accredify
Ms Elsie Tan	Country Manager Worldwide Public Sector, Singapore at Amazon Web Services (AWS)
Mr Eoin Fleming	Chief Information Officer, Carnel Group
Mr Henry Quek	Deputy Director (Resilience Cybersecurity Policy & Planning), IMDA
Mr Huang Shaofei	Fellow, Singapore Computer Society Cybersecurity Chapter, Association of Information Security Professionals
Mr Ichiro Seino	Regional Automotive Industry Leader, Marsh Asia
Ms Indra Suppiah	Government Relations Lead – APAC, R3
Ms Jane Lim	Deputy Secretary (Trade), Ministry of Trade and Industry (Singapore)
Mr Jeth Lee	Director of Legal and Government Affairs, Microsoft
Ms Katharine Jarmul	Principal Data Scientist, Thoughtworks
Mr Ken Chua	Group Deputy Director, FinTech Infrastructure Office, FinTech and Innovation Group, MAS
Mr Kenneth Siow	General Manager for Singapore, Malaysia & Indonesia and Regional Director SEA, Tencent Cloud International
Mr Kiat Lim	Privacy Engineer, Google
Dr Konstantinos Komaitis	Senior Director, Policy and Development, Internet Society
Dr Kuo-yi Lim	Co-Founder & Managing Partner, Monk's Hill Ventures

Expert Interviewees (continued)

Mr Lawrence Goh	Managing Director and COO of Group Technology & Operations, UOB Group
Prof Lam Kwok Yan	Executive Director, the Strategic Centre for Research in Privacy-Preserving Technologies and Systems (SCRiPTS), NTU
Mr Lee Ser Yen	Partner, Cybersecurity, KPMG
Ms Lien Huiluen	Director, Marketing and Strategic Partnerships, Sensetime
Mr Lih Shiun Goh	Senior Director for Public Affairs, Tencent
Mr Linden Reko	Cyber Advisor - Cyber Practice Asia, Marsh
Ms Lisa Mansour	Director, Product Management (Consulting, Insights & Analytics, Data Management), Mastercard
Mr Lokesh Bangalore	Vice President, Security and Compliance, Salesforce
Mr Lucius Lee	Senior Policy Lead, Product and Content, Aaqua
Admiral Mike Rogers	Senior Advisor, Brunswick Group
Dr Ming Tan	Founding Executive Director, Tech for Good Institutes
Mr Minn Naing Oo	Managing Director and Partner, Allen & Gledhill
Mr Nabil Hamzi	Chief Product Security Architect, Logitech
Mr Nicholas Fang	Managing Director, Black Dot Research
Mr Nick Pan	Head of Recruitment, Tik Tok
Mr Paddy McGuiness, CMG OBE	Senior Advisor, Brunswick
Mr Rajat Maheshwari	Vice President, Digital Identity and Biometrics, Mastercard
Mr Rajeev Tummala	Director, Digital & Data, Markets & Securities Services, HSBC
Dr Raymond Chan	Expert AIOps Engineer, SAP
Mr Raymund Liboro	Commissioner and Chairman, National Privacy Commission (Philippines)
Mr Shameek Kundu	Head of Financial Services and Chief Strategy Officer, Truera
Prof Simon Chesterman	Dean, Faculty of Law, National University of Singapore
Mr Simon Gordon	Chief Commercial Officer, Accredify
Ms Siobhan Gorman	Partner, Crisis, Cybersecurity, Public Affairs and Media Relations, Brunswick Group
Mr Steven Koh	Director, Government Digital Services, GovTech
Ms Sunitha Chalam	Partner, Cybersecurity & Data Privacy Asia Pacific Lead, Brunswick Group
Mr Thomas Tay	Assistant Director, Product, IMDA
Mr Traven Teng	International Talent Acquisition Lead, Tencent
Ms Veronica Tan	Director, Safer Cyberspace, CSA
Ms Wan Wei Soh	Co-Founder & CEO, IKIGUIDE Metaverse Collective
Ms Wendy Lim	Partner, Cybersecurity Consulting, KPMG
Prof Jason Yap Chin Huat	Dean & Vice Provost, Practice, NUS
Mr Yeong Zee Kin	Deputy Commissioner, Personal Data Protection Commission
Ms Yvonne Lim	Director, Business and Ecosystems, IMDA

We would also like to put on record our thanks to the following organisations for supporting this study: Enterprise Singapore; our Presenting Sponsors Amazon Web Services (AWS) and NetSfere; our supporting sponsors Intel, Lenovo and Microsoft; and Eden Strategy Institute for their dedicated support in the industry consultation and research process.

12 References

[1]Infocomm Media Development Authority (IMDA). (2020). *Singapore grows trust in the digital environment.* Retrieved from https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2022/Singapore-grows-trust-in-the-digital-environment

[2]Personal Data Protection Commission Singapore (PDPC). (2020). *Model Artificial Intelligence Governance Framework Second Edition.* Retrieved from https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2022/Singapore-grows-trust-in-the-digital-environment

[3]POFMA Office. (2019). *Protection from Online Falsehoods and Manipulation Act (POFMA).* Retrieved from https://www.pofmaoffice.gov.sg/regulations/protection-from-online-falsehoods-and-manipulation-act/

[4]PDPC Singapore. (n.d.). *Data Protection Officers.* Retrieved from https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-officers

[5]GovTech Singapore. (2021). *All Government Agencies to Accept Singpass Digital IC from 1 November 2021.* Retrieved from https://www.tech.gov.sg/media/media-releases/2021-10-28-all-government-agencies-to-accept-singpass-digital-ic-from-1-november-2021

[6]The Association of Banks in Singapore (ABS). (2021). *Data Sharing Handbook: For Banks and Non-Bank Data Ecosystem Partners.* Retrieved from https://www.tech.gov.sg/media/media-releases/2021-10-28-all-government-agencies-to-accept-singpass-digital-ic-from-1-november-2021

[7]Ritter, J. (2019). *What is digital trust?* Tech Target. Retrieved from https://www.techtarget.com/whatis/definition/digital-trust

[7]Chakravorti, B., Bhalla, A., & Chaturvedi, R. (2018). *The 4 Dimensions of Digital Trust, Charted Across 42 Countries.* Harvard Business Review. Retrieved from https://hbr.org/2018/02/the-4-dimensions-of-digital-trust-charted-across-42-countries

[7]PricewaterhouseCoopers (PWC). (2019). *The Journey To Digital Trust 2019* [E-book]. Retrieved from https://www.pwc.com/sg/en/publications/assets/the-journey-to-digital-trust-2019.pdf

[7]World Economic Forum (WEF). (2022). *Digital Trust.* Retrieved from https://www.weforum.org/projects/digital-trust

[7]Klynveld Peat Marwick Goerdeler (KPMG). (2015). *What is Digital Trust* [E-book]. Retrieved from https://assets.kpmg/content/dam/kpmg/pdf/2015/12/digital-trust.pdf

[7]Raviprakash, R. (2020). *What is Digital Trust?.* Subex Limited. Retrieved from https://www.subex.com/blog/what-is-digital-trust/

[7]Allan, A., Zlotogorski, M., Gaehtgens, F., & Buytendijk, F. (2017). *Definition: Digital Trust.* Retrieved from https://www.gartner.com/en/documents/3727718/definition-digital-trust

[7]Hitachi. (2020). *Understanding Digital Trust.* Retrieved from https://www.hitachi.com/rd/sc/ai-analytics/003/index.html.

[7]Swinhoe, D. (2018). *What is digital trust?* How CSOs can help drive business. Retrieved from https://www.csoonline.com/article/3297037/what-is-digital-trust-how-csos-can-help-drive-business.html

[7]ISACA. (2022). *State of Digital Trust 2022*. Retrieved from https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/reports/state-of-digital-trust-2022-report-final.pdf

[7]Zahn, N., & Paeffgen, N. (2022). *Digital Trust Whitepaper. Swiss Digital Initiative.* Retrieved from https://a.storyblok.com/f/72700/x/7bd8e2fe21/digital-trust-whitepaper.pdf

[8]Shuklar, A.K. (2021). *India leads the global e-governance race with 1.3 bn digital ID users.* Economic Times (ET) Government. Retrieved from https://government.economictimes.indiatimes.com/news/digital-india/india-leads-the-global-e-governance-race-with-1-3-bn-digital-id-users/90789137

[9]European Parliamentary Research Service (EPRS). (2022). *Updating the European digital identity framework.* Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698772/EPRS_BRI(2021)698772_EN.pdf

[10]Zheng, W. (2022). *China plans digital version of national identification card later this year, premier says.* South China Morning Post (SCMP). Retrieved from https://www.scmp.com/news/china/politics/article/3170214/china-plans-digital-version-national-identification-card-later

[11]Edelman Research. (2022). *Edelman Trust Barometer 2022* [E-book]. Retrieved from https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022%20Edelman%20Trust%20Barometer%20FINAL_Jan25.pdf

[12]Edelman Research. (2021). *Edelman Trust Barometer 2021* [E-book]. Retrieved from https://www.edelman.com/sites/g/files/aatuss191/files/2021-03/2021%20Edelman%20Trust%20Barometer.pdf

[13]Edelman Research. (2021). Edelman Trust Barometer 2021 [E-book]. Retrieved from https://www.edelman.com/sites/g/files/aatuss191/files/2021-03/2021%20Edelman%20Trust%20Barometer.pdf

[14]Imperva. (2022). *Imperva Bad Bot Report* [E-book]. Retrieved from https://www.imperva.com/resources/reports/2022-Imperva-Bad-Bot-Report.pdf

[15]Ipsos. (2019). *CIGI-IPSOS Global Survey: Internet Security & Trust, 2019 Part 3: Social Media, Fake News & Algorithms.* [E-book]. Retrieved from https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey%20-%20Part%203%20Social%20Media%2C%20Fake%20News%20%26%20Algorithms.pdf

[16]Tandoc, E., Goh, Z., & Lee, E. (2022). *Digital Life During a Pandemic, Results from a Panel Study.* Nanyang Technological University Singapore. Retrieved from https://www.ntu.edu.sg/docs/librariesprovider127/default-document-library/in-cube-working-paper-no.1.pdf?sfvrsn=442c20003

[17]Ipsos. (2019). *CIGI-IPSOS Global Survey: Internet Security & Trust, 2019 Part 3: Social Media, Fake News & Algorithms.* [E-book]. Retrieved from https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey%20-%20Part%203%20Social%20Media%2C%20Fake%20News%20%26%20Algorithms.pdf

[18]Imperva. (2022). *Imperva Bad Bot Report* [E-book]. Retrieved from https://www.imperva.com/resources/reports/2022-Imperva-Bad-Bot-Report.pdf

[19]POFMA Office. (2019). *Protection from Online Falsehoods and Manipulation Act (POFMA)*. Retrieved from https://www.pofmaoffice.gov.sg/regulations/protection-from-online-falsehoods-and-manipulation-act/

[20]Confessore, N. (2018). *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far.* The New York Times. Retrieved from https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

[21]Buranyi, S. (2017). *Rise of the racist robots – how AI is learning all our worst impulses.* The Guardian. Retrieved from https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses

[22]United Nations Conference on Trade and Development (UNCTAD). (n.d.). *Data Protection and Privacy Legislation Worldwide.* Retrieved from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[23]United Nations Conference on Trade and Development (UNCTAD). (2021). *Data Protection and Privacy Legislation Worldwide.* Retrieved from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[24]China Briefing (2021). *The PRC Personal Information Protection Law (Final): A Full Translation.* Retrieved from https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/

[25]SC Media (2022). *California Privacy Rights Act (CPRA) compliance checklist: What you need to know.* Retrieved from https://www.scmagazine.com/native/incident-response/california-privacy-rights-act-cpra-compliance-checklist-what-you-need-to-know

[26]Singapore Computer Society (2020). *AI Ethics and Governance Body of Knowledge.* Retrieved from https://www.scs.org.sg/ai-ethics-bok

[27]The Organisation for Economic Co-operation and Development (OECD) (2022). *OECD AI's Live Repository of AI Strategies & Policies.* Retrieved from https://oecd.ai/en/dashboards

[28]United Nations Conference on Trade and Development (UNCTAD). (2021). *Data Protection and Privacy Legislation Worldwide.* Retrieved from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[29]Cavoukain, A. (2011). *Privacy by Design, The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices.* Information and Privacy Commissioner of Ontario. Retrieved from https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

[30]Morgan, S. (2020). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025.* Cybercrime Magazine. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[31]Morgan, S. (2019). *Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021. Cybercrime Magazine.* Retrieved from https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

[32]Wilkie, C. (2021). *Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate.* CNBC. Retrieved from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[33]Check Point Software. (2021). *Check Point Research: Asia Pacific experiencing a 168% year on year increase in cyberattacks in May 2021.* Retrieved from https://blog.checkpoint.com/2021/05/27/check-point-research-asia-pacific-experiencing-a-168-year-on-year-increase-in-cyberattacks-in-may-2021/

[34]Statista Research Department. (2022). *Cybercrime as a share of total crimes in Singapore from 2014 to 2021.* Retrieved from https://www.statista.com/statistics/1267252/singapore-cybercrime-as-share-of-total-crime/#:~:text=Cybercrime%20as%20share%20of%20total%20crime%20Singapore%202014%2D2021&text=In%202021%2C%20-cybercrime%20made%20up,crimes%20committed%20in%20the%20country

[35]Morgan, S. (2020). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025.* Cybercrime Magazine. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[36]Walter, J. (2020). *COVID-19 News: FBI Reports 300% Increase in Reported Cybercrimes.* IMC Grupo. Retrieved from https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/

[37]Check Point Software. (2021). *Check Point Research: Asia Pacific experiencing a 168% year on year increase in cyberattacks in May 2021.* Retrieved from https://blog.checkpoint.com/2021/05/27/check-point-research-asia-pacific-experiencing-a-168-year-on-year-increase-in-cyberattacks-in-may-2021/

[38]Ganesan, N. (2022). *Singapore faced more cybercrime, phishing and ransomware threats in 2021.* Channel News Asia (CNA). Retrieved from https://www.channelnewsasia.com/singapore/cybercrime-ransomware-phishing-cybersecurity-2021-2906386

[39]Cyber Security Agency of Singapore (CSA). (2022). *Cyber Trust Mark*. Retrieved from https://www.csa.gov.sg/Programmes/sgcybersafe/cybersecurity-certification-for-enterprises/cyber-trust-mark

[40]Cory, N. & Dascoli, L. (2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them* [E-book]. Information Technology & Innovation Foundation. Retrieved from https://www2.itif.org/2021-data-localization.pdf

[41]Cory, N. & Dascoli, L. (2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them* [E-book]. Information Technology & Innovation Foundation. Retrieved from https://www2.itif.org/2021-data-localization.pdf

[42]Yan, L., Yu, Z., & Liu, V. (2021). *The future of data localization and cross-border transfer in China: a unified framework or a patchwork of requirements?* Financial Crimes Enforcement Network. Retrieved from https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act

[43]Greenwalf, G., MacAskill, E., & Poitras, L. (2013). *Edward Snowden: the whistleblower behind the NSA surveillance revelations.* The Guardian. Retrieved from https://www.theguardian.com/world/2013/jun/09/Edward-snowden-nsa-whistleblower-surveillance

[44]Financial Crimes Enforcement Network. (n.d.). *USA Patriot Act.* Retrieved from https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act

[45]International Association of Privacy Professionals (IAPP) & Ernst & Young (EY) (2021). *IAPP-EY Annual Privacy Governance Report 2021* [E-book]. Retrieved from https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf

[46]IAPP & EY. (2021). IAPP-EY Annual Privacy Governance Report 2021 [E-book]. Retrieved from https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf

[47]Association of Southeast Asian Nations (ASEAN). (2021). *ASEAN Model Contractual Clauses for Cross Border Data Flows.* Retrieved from https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

[48]Finlayson-Brown, J. (2022). *New Global Cross-Border Privacy Rules Forum established by APEC CBPR members.* Allen & Overy. Retrieved from https://www.allenovery.com/en-gb/global/blogs/digital-hub/new-global-cross-border-privacy-rules-forum-established-by-apec-cbpr-members

[49]Mastercard. (2019). *Restoring Trust in a Digital World.* Retrieved from https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf

[50]Bank for International Settlements (BIS). (2022). *Project Dunbar: International settlements using multi-CBDCs.* Retrieved from https://www.mas.gov.sg/-/media/MAS-Media-Library/development/fintech/Dunbar/Project_Dunbar_Report_2022.pdf

[51]Association of Southeast Asian Nations (ASEAN). (2021). *2021 ADGSOM Project Completion Report: Blockchain for digital government – the ASEAN way* [E-book]. Retrieved from https://asean.org/wp-content/uploads/2022/02/02-Final-_-Report-Blockchain-for-digital-government.pdf

[52]Bigg, C., Lee, Y. L., & To, G. (2022). *Singapore: Higher Fines for Breach of Personal Data Protection Act 2012 (PDPA) – up to 10% of Singapore Turnover.* Bank for International Settlements (BIS). Retrieved from https://blogs.dlapiper.com/privacymatters/singapore-higher-fines-for-breach-of-personal-data-protection-act-2012-pdpa-up-to-10-of-singapore-turnover/

[53]Wolford, B. (2019). *What are the GDPR Fines?* GDPR.eu. Retrieved from https://gdpr.eu/fines/

[54]Morgan, S. (2021). *Cybersecurity Jobs Report: 3.5 Million Openings In 2025.* Cybercrime Magazine. Retrieved from https://cybersecurityventures.com/jobs/

[55]Polaris Market Research (2021). *Enterprise Governance, Risk & Compliance Market Share, Size, Trends, Industry Analysis Report, By Component (Software, Services); By Software (Audit Management, Compliance Management, Risk Management, Policy Management, Incident Management, Others); By Services; By Vertical; By Region; Segment Forecast, 2021 – 2028.* Retrieved from https://www.polarismarketresearch.com/industry-analysis/enterprise-governance-risk-compliance-egrc-market

[56]International Data Corporation (IDC) (2021). *IDC Forecasts Solid Growth for GRC Solutions as Enterprises Invest to Expand and Integrate Their Governance and Risk Management Portfolios.* Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS48171921

SGTech, which celebrated its 40th anniversary in 2022, is the leading trade association for Singapore's tech industry. Representing over 1,000 member companies ranging from top multinational corporations, large local enterprises, vibrant small and medium-sized enterprises, and innovative startups, it is the largest community in Singapore where companies converge to advocate for change and drive what enables tech innovation and accelerates tech adoption to spur greater sustainability in the sector.

SGTech's mission is to catalyse a thriving ecosystem that powers Singapore as a global tech powerhouse.

Get in Touch

SGTech - through its Digital Trust Committee - is spearheading many initiatives towards positioning Singapore as a global node for digital and data, built on trust. Interest in our work on Digital Trust among our membership is growing rapidly and we welcome collaboration from all stakeholders in the tech ecosystem, whether from industry, government or the non-profit sector.

Contact us if you would like to learn more on how to be part of our Digital Trust journey, or if you wish to find out more about the complete Digital Trust Landcape Study.

research@sgtech.org.sg

sgtech.org.sg
SGTech
SGTech
research@sgtech.org.sg