Published by:

SGTECH
WHERE TECH MEETS

DIGITAL TRUST REPORT

MAY 2025



1 FOREWORD

Digitalisation is drastically reshaping the business landscape in Singapore. Digital Trust, the confidence of participants to interact securely and transparently within this growing digital ecosystem, serves as a crucial foundation only upon which businesses can effectively capture growth opportunities and mitigate ever-evolving threats.

Due to the immense scope and scale of digitalisation, coupled with the inextricable fusion of technology within most job functions, the onus to preserve and develop this sacred commodity has since exceeded the confines of domain-experts and internal policy teams. This report seeks to provide business owners and employees with an overview of Digital Trust's implications across the workforce, most particularly on tech-enabled roles. More importantly, it should serve as a practical guide for business owners to prepare their employees for the increasingly digital world.

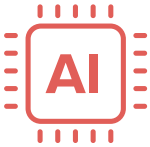


2 EXECUTIVE SUMMARY

Digital Trust is the "confidence participants have in the digital ecosystem to interact securely, in a transparent, accountable and frictionless manner."[1] Digital technology pervades almost every aspect of our lives, but the orderly functioning of a digital economy requires Digital Trust. That, in turn, means that the workforce needs to build their Digital Trust skillset.

Most individual components of the Digital Trust skillset are not new. However, the growing importance of Digital Trust means that greater emphasis needs to be placed on building these skills as a coherent set in a far greater proportion of the workforce than most people realise. In fact, we argue that it should be seen as a new competency that many workers will need.

The Digital Trust skillset focuses on 4 areas:



Artificial Intelligence



Business Resilience



Cyber Security



Data Protection

[1] SGTech Whitepaper - "Digital Trust - Unlocking the Next Wave of Growth in the Digital Economy", 2022

As technology adoption and digitalisation continue to accelerate, it is essential to recognise that the 4 pillars are inter-connected, and you need to know all of them to build and protect Digital Trust. Hence, these skills should be taught as a set to build Digital Trust competency.

The other key insight is that these skills are not only relevant for 'tech workers', but all workers who use technology as part of their work. These 'Tech-enabled Workers' are present in all companies, performing roles such as Product management, HR, Finance, Communications. They may not think of themselves as 'tech', but play a critical role in protecting Digital Trust, and hence need the Digital Trust skillset.



Taken together, these insights lead to the conclusion that SMEs need to urgently equip their workforce with Digital Trust skills as part of their digitalisation journey. While there has been upskilling of staff, these have often focused on enabling them to use the new technologies effectively. SMEs need to tap skills programs such as Career Conversion Programs (CCP), SkillsFuture Enterprise Credits (SFEC) and others to build Digital Trust skills in all their Tech-enabled Workers.

To support SMEs, the skills ecosystem also needs to work together to ensure that Tech-enabled Workers have access to the Digital Trust training they need. Government agencies like Skillsfuture Singapore (SSG) and the Infocomm Media Development Authority (IMDA) need to catalyse the ecosystem to act. Training providers need to translate the Digital Trust skillset into compelling training programs. This will help companies, especially SMEs, with their upskilling journeys.

3 WHAT IS DIGITAL TRUST

Digital technology pervades almost every aspect of our lives, but the orderly functioning of a digital economy requires Digital Trust. This important concept was the focus of SGTech's Whitepaper on Digital Trust in 2022, and further expanded upon in The Digital Trust Workforce Global Edition in 2024.

What do we mean by Digital Trust?

Digital Trust is the "confidence participants have in the digital ecosystem to interact securely, in a transparent, accountable and frictionless manner".[2] Without this, participants - be they consumers, employees, job applicants or any other stakeholder - may become unwilling to perform digital transactions, and the digital economy would grind to a halt. Given that Singapore's digital economy is expected to grow to SGD 765B in 2027,[3] this loss would be catastrophic.

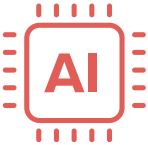
Building Digital Trust requires a combination of technology, infrastructure, and the right governance and policies. Crucially, it also requires a workforce that has the necessary skills to maintain and reinforce Digital Trust. This goes beyond what would traditionally be considered tech or cybersecurity skills, and is not limited just to 'tech' roles. Instead, it requires a balance of technical and softer business and interpersonal skills.[4]

What are the 5 pillars of Digital Trust?



Artificial Intelligence | **B**usiness Resilience | **C**yber Security | **D**ata Protection | **E**merging Issues

[2] SGTech Whitepaper - "Digital Trust - Unlocking the Next Wave of Growth in the Digital Economy", 2022
[3] SGTech Whitepaper - "Digital Trust - Unlocking the Next Wave of Growth in the Digital Economy", 2022
[4] SGTech: The Digital Trust Workforce: Global Edition, 2024



Artificial Intelligence (AI)

Artificial Intelligence (AI) is fast becoming embedded in how companies operate. From Machine Learning to Generative AI, it is almost impossible to avoid using some form of AI at work. However, a tool as powerful as AI needs to be used correctly and responsibly. Hence, ensuring that AI is used within responsible and ethical guardrials is a necessary component of Digital Trust.



Business Resilience

From a Digital Trust perspective, **Business Resilience** requires that companies are effective in preventing, detecting, and responding to technology disruptions. While disruptions can also come from non-digital sources, the focus here is on rapid identification and mitigation of digital threats to minimise disruption to business operations, and hence limiting any damage to Digital Trust in a company.



Cybersecurity

Cybersecurity is the protection of digital systems and networks against threats, which could lead to consequences such as information or data disclosure or the disruption or misdirection of services. With bad actors constantly searching for vulnerabilities or new methods of attack, companies need to remain at the forefront of cybersecurity to maintain Digital Trust.[5]



Data Protection

Data Protection is the fourth pillar of Digital Trust, and refers to the range of steps companies need to take to safeguard the privacy, availability, and integrity of sensitive data. The specific regulations that apply to data may vary by geography and type of data, but protecting and securing data are essential for maintaining Digital Trust.[6]



Emerging issues

Given the rapid advances in technology, we have included **Emerging Issues** as the final pillar. This reminds everyone involved in Digital Trust that they need to remain constantly vigilant, and react rapidly to new threats as they emerge - maintaining the status quo will not be enough.

[5] Alternative Definition from CSA: Cybersecurity means the state in which a computer or computer system is protected from unauthorised access or attack, and because of that state — the computer or computer system continues to be available and operational; the integrity of the computer or computer system is maintained; and the integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained

[6] Alternative Definition from IBM: Data protection is the practice of safeguarding sensitive information from data loss and corruption. Its goal is to protect data and ensure its availability and compliance with regulatory requirements.

Building and growing Digital Trust requires multiple parties to work together seamlessly and continuously - the ecosystem is only as strong as its weakest link. Given the breadth of the Digital Trust ecosystem, it requires that almost every member of the workforce play a role. This in turn means that the workforce will need to be upskilled. We look at this in the next chapter.



4 DIGITAL TRUST IMPLICATIONS FOR THE WORKFORCE

What does the rising importance of Digital Trust mean for the workforce?

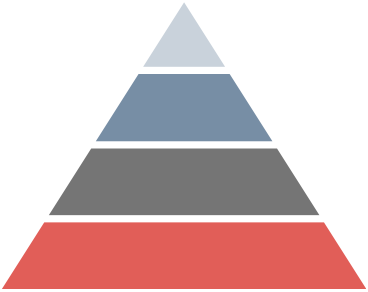
The implications of Digital Trust will differ for different segments of the workforce.

- **Technical Specialists** are technical experts who build the solutions, ranging from new AI functionalities to enhanced cybersecurity tools, that form the basis of Digital Trust, e.g., software engineers, cybersecurity analyst, etc.

- **Internal Policy Managers** are leaders within each firm who set up and update their Digital Trust policies and guidelines. These include roles such as CISO, CIO, CTO, Chief Privacy Officer, but also more general digital business roles, such as CHRO, Chief Compliance Officer or Marketing Director.[7]

- **Tech-enabled Workers** are those employees who rely on technology to perform their tasks, even if they do not see themselves as "tech workers". This includes most corporate and revenue generating functions, such as HR, finance, sales/marketing, product, and communications

- **General Workers** are the rest of the workforce who do not primarily use technology, but still have a role to play in protecting Digital Trust



1.Technical specialists
Develop and implement digital trust solutions

2.Policy Managers
Develop digital strategy, policies, and processes

3.Tech-enabled Workers
Directly access and leverage data as part of their tasks (e.g. HR, finance)

4.General
Possess incidental access to data and are connected to the company's digital ecosystem

[7] SGTech: The Digital Trust Workforce: Global Edition (2024)

Technical Specialists and **Internal Policy Managers** bear the greatest burdens of building and maintaining Digital Trust. However, they will not be the focus of this report, as these groups will typically require more specialised technical skills. These groups are also relatively small in number, both as a proportion of the total workforce, and within each company. It is also usually clear, based on their distinct job titles/functions, that they will need to be Digital Trust specialists. Hence these two groups would be best placed to identify their own specific skill requirements, and work with specialists to develop relevant training programs.

In this report, we focus primarily on **Tech-enabled Workers** and the Digital Trust skills they will need to acquire. There are 4 key reasons for this focus:

- Tech-enabled workers are a large proportion of the workforce, and rapidly growing in number as companies digitalise
- Tech-enabled workers exist in every company, performing essential corporate functions
- Tech-enabled workers can significantly damage Digital Trust if they make mistakes, due to their access to data and systems
- Tech-enabled workers typically do not see themselves as tech workers and hence are less likely to be aware of the importance of Digital Trust skills



Tech-enabled Workers will continue to grow as a proportion of the workforce, as 'traditional' job roles are increasingly being digitally transformed. Given their job scopes, without the right skills, mistakes made by such workers could have potentially catastrophic impacts on Digital Trust. Hence it is critical to articulate the Digital Trust skillset Tech-enabled Workers require, and curate upskilling programs to help them acquire essential skills.

Many of the same Digital Trust skills, knowledge or abilities identified for Tech-enabled Workers will also be applicable to General Workers. Typically, General Workers will require a more basic knowledge of these skills.



In the next chapter, we synthesise the 5 common focus areas that are part of most Tech-enabled Workers' roles, in order to identify a set of core Digital Trust skills that almost all of them will require. This will form the starting point for companies that are looking to build Digital Trust capabilities across their workforce. Where feasible, General Workers should also be provided with elements of this set of core Digital Trust skills, as appropriate for their role and function.

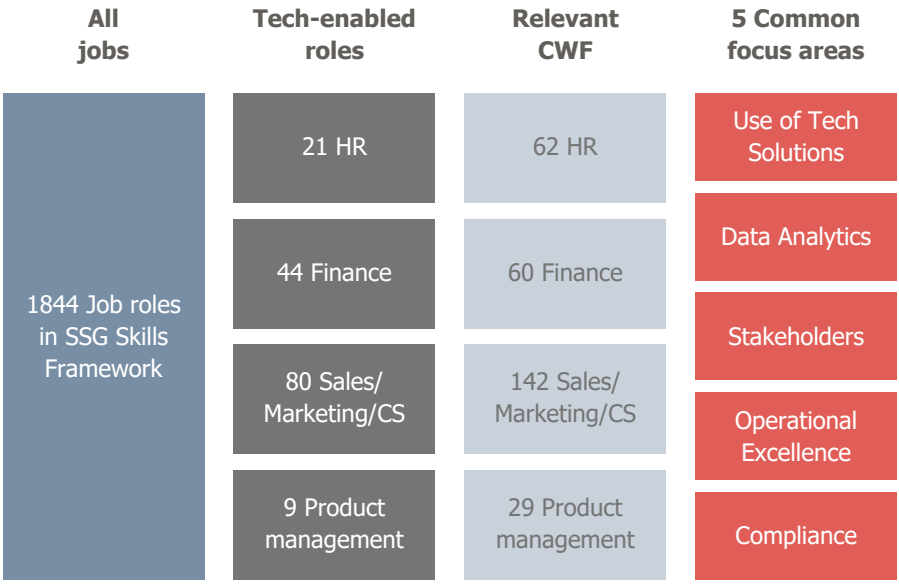
5 DEEP-DIVE INTO SKILLS IMPLICATIONS FOR TECH-ENABLED ROLES

Who are Tech-enabled Workers, and what do they do?

We examined the 1844 job roles listed in the Singapore Skills Framework compiled by Skillsfuture Singapore, and identified over 154 tech-enabled roles that are present in most organisations. These include roles related to:

- **Finance and Accounting**
- **Human Resources**
- **Sales, Marketing and Customer Relations**
- **Product and Revenue Management**

We then compiled the 294 Critical Work Functions associated with these roles, and sifted through them systematically. This enabled us to identify 5 common focus areas for Tech-enabled Workers.





Use of technology solutions

The biggest difference between Tech-enabled Workers and their predecessors is the fact that they now need to be proficient in the use of technology solutions in a way that previous generations did not. As companies have digitalised and automated processes that used to be paper-based and manual, use of technology, including Generative AI, has become a common focus area of the functions that Tech-enabled Workers perform within their companies.



Data management

In tandem with greater digitisation, which makes more data easily available, most functions have seen a rise in the use of data management. Corporate functions are increasingly expected to provide quantitative insights to support their decision-making. Data management is therefore now another common focus area for Tech-enabled Workers.



Stakeholder management

Working with other people has always been at the core of most corporate functions. These stakeholders can be internal, such as employees, or they can be external, such as customers, partners, vendors, investors, etc. Technology has changed how Tech-enabled Workers communicate with stakeholders and store their information, but it has not eliminated the need to manage them, and this remains a common focus area for many roles.



Operational excellence

Tech-enabled Workers are expected to deliver the best possible outcomes - be it in terms of customer/employee satisfaction, cost, time, etc. Beyond that, they are also expected to identify opportunities for improvement, through use of technology, process redesign, upskilling, etc. Therefore, operational excellence is a common focus area for most Tech-enabled Workers.



Compliance

Given that most Tech-enabled Workers have corporate functions, they will typically be responsible for ensuring compliance with the relevant regulations in their field. This could include Financial Reporting standards, Occupational Health and Safety rules, or rules around information disclosure for investors. Some of them will compile compliance reports for the authorities, but even those that do not will need to know and comply with the rules, making Compliance the fifth common focus area for Tech-enabled Workers.

As has been shown above, these five common focus areas capture essential elements of what Tech-enabled Workers do. We are not claiming that all Tech-enabled Workers perform all five of these focus areas, or that these focus areas fully describe everything that they need to do. Instead, they are meant to provide a collective starting point to identify the Digital Trust skills Tech-enabled Workers will need, regardless of their specific specialised function or industry.



	AI	Business Resilience	Cyber-security	Data Protection	Emerging threats
Using of Tech Solutions	✓	✓	✓		To be defined
Data management	✓			✓	
Stakeholders	✓	✓		✓	
Operational excellence	✓	✓			
Compliance	✓	✓	✓	✓	

AI skills for Tech-enabled Workers

The increasing pervasiveness of AI, including GenAI, means that all Tech-enabled workers will need to be able to work effectively with it, in a manner that does not compromise Digital Trust. Most workers will not be involved in highly-technical activities such as training models - that is left to Technical Specialists. However, all workers who use AI will need to know the foundations , so that they do not accidentally damage Digital Trust in their organisation while using AI tools. While some customisation will be required on the specific AI use case being discussed, this skill applies across all 5 common focus areas.

While there are different definitions for **Ethical AI**, our focus here is on 3 of the 5 pillars identified by IBM[8], which focuses on the practical applications to reduce risk

- Fairness - users should avoid inequitable treatment of individuals, or groups of individuals, as a result of using AI tools
- Data Privacy - users should prioritise and safeguard the privacy of data that is being provided to the AI tool
- Transparency - users should know how an AI tool works, evaluate its functionality, and comprehend its strengths and limitations

We can think of a generalised model of AI usage with 4 stages



1. Input - preparing the dataset
2. Processing - turning the input data into output
3. Output - verifying the output of the AI tool
4. Actions taken - translating output into tangible actions

[8] https://www.ibm.com/think/topics/ai-ethics

The role for Tech-enabled Workers is to ensure that they uphold the pillars of Ethical AI throughout the 4 stages.

Input	Processing	Output	Actions taken
Confirm that input dataset meets the **data privacy** standards	Ensure data provided is **fair**, i.e., accurate and representative	Verify output for violations of **fairness**	Check that actions taken based on AI output are **fair**
Maximise likelihood of **fair** and accurate results by entering the right prompts	Provide **transparency** by being able to explain it to stakeholders	Verify whether output violates **privacy** and confidentiality of personal/ company data	Raise concerns to tech/devt teams to maintain **transparency**

Ethical AI is applicable to all 5 common focus areas for Tech-enabled Workers, regardless of function. As AI and GenAI become more pervasive in the workplace, it becomes increasingly important that all Tech-enabled workers have this base level of knowledge. It should be sufficient in most cases, but, of course, some specific use cases may have additional requirements in order to prove fairness or transparency.

Business Resilience

With the accelerating trend of digitalisation of systems and processes across multiple work functions increasing businesses' reliance on key digital infrastructure and networks, Tech-enabled Workers will find themselves playing a crucial role in the maintenance of Business Resilience should things go wrong.

We can think about the knowledge and abilities Tech-enabled Workers will need in order to manage disruption without eroding Digital Trust in 3 phases.

- Prevention - Precluding lapses and points of failure
- Detection - Recognition and escalation of failure
- Response - Maintain critical operations during disruption and expedite recovery process

Prevention	Detection	Response
Adapt and adhere to company's newest standard operating procedures	Recognise symptoms of failure	Communicate to external stakeholders (regulators, customers, investors)
Participate in tabletop exercises to help management identify points of failure in the overall operational resilience strategy	Practice rapid and timely reporting to the relevant management team for activation of whole-of-enterprise response plan	Execute company's business continuity and crisis management plan

While different roles may require these skills to different extents, these competencies will be critical to help Tech-enabled Workers to safeguard Digital Trust.

Cybersecurity

Cybersecurity is the protection of digital systems and networks against threats. This happens at multiple levels. Strategic and technological decisions, such as choice of software or security policies, are the responsibility of Technical Specialists and Policy Managers within each organisation. However, all Tech-enabled Workers have a role to play, given that they have access to essential systems. At a minimum, they need to practice **Cyber Hygiene**, building on the existing skills of Cyber and Data Breach Incident Management and Infocomm Security and Data Privacy.

Tech-enabled Workers will need to be taught the principles of good Cyber Hygiene in order to protect Digital Trust. They also need to be able to comply with company cybersecurity protocols, to prevent creating entry points for malicious actors to launch cyberattacks. Given that they work first-hand with essential systems, Tech-enabled workers should also be equipped to facilitate rapid detection of breaches and, where possible, take preventative measures within their power to ensure a breach does not spread further.

By definition, all Tech-enabled Workers use technology to perform their jobs, hence all of them will need to acquire **Cyber Hygiene** as a Digital Trust skill. **Cyber Hygiene** will also be relevant to General Workers who have access to core systems, since they could also be points of vulnerability within the system.

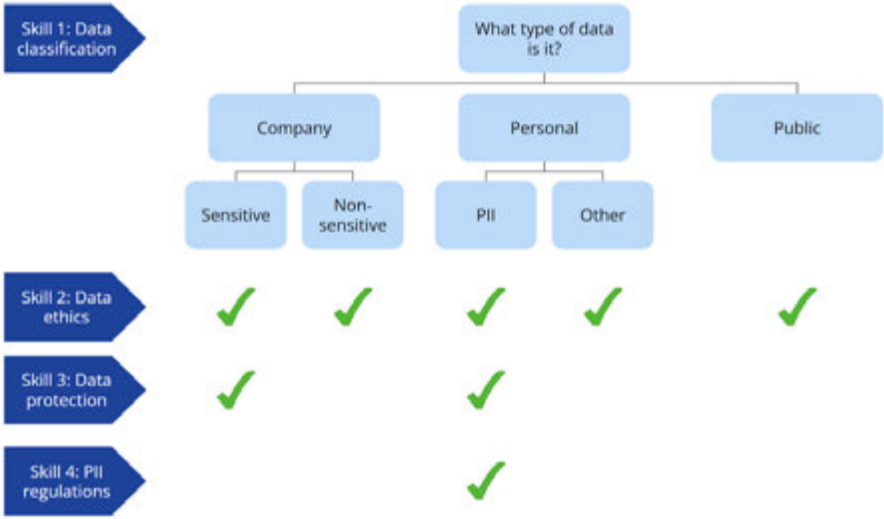


Data protection

Data protection becomes increasingly important as the volume and types of data being stored and processed continues to rise. Many Tech-enabled Workers will come into contact with data of various forms, and hence need to contribute to data protection.

Tech-enabled workers may work directly with the analysis of data, or they may come into possession of data as part of their work, for example, employee or customer data. Others may also be involved in compliance functions, compiling information for regulators. The data-related skills they require include:

- **Data classification:** ability to sort data by type, level of sensitivity, etc.
- **Data ethics:** ensuring that data is used in the right way
- **Data protection:** physical safeguarding of data (cybersecurity of data is part of cyber)
- **Data regulation:** ensuring compliance with specific regulations for various types of data, such as Personally Identifiable Data (PII)



Emerging Threats

Even as new digital applications and benefits are constantly being developed, emerging threats are always lurking. For Tech-enabled Workers, this can take the form of ingenious new scams or deceptive practices that try to exploit any vulnerability within the system. Therefore it is essential that Tech-enabled Workers embrace **lifelong learning and resilience**. Challenges and mistakes will happen, but with the right process in place, the impact should be limited, and hence they need to be seen as opportunities to improve. Maintaining Digital Trust will require an evolving set of skills, and Tech-enabled Workers should view the time and effort spent on upskilling as a benefit, not a chore.



6 CASE STUDIES

Data management + AI

E-commerce Giant

An E-commerce giant designed an AI system to impartially and automatically sift through resumes and select the top candidates. However, the system was found to have a negative bias against women for software development and other technical positions. This bias stemmed from the overrepresentation of male applicants in the training dataset. In the past, the majority of previous successful applications came from men. In this way, HR professionals unwittingly perpetuated male overrepresentation in the tech industry. This result caused a public uproar once revealed. It undermined the public's trust and confidence in said company's data analytic tools and processes.



Stakeholders + Data Protection/Cybersecurity

Effective stakeholder management is becoming increasingly important. This is due to the rise in stakeholder data and growing digital risks threatening business operations. The following cases highlight potential risks associated with poor stakeholder management.

Professional network

An Irish Data Protection Commission (DPC) investigation revealed that employees at a global professional network inadequately informed data subjects about their firm's intention to process customer data for behavioral analysis and targeted advertising. This lack of communication violated GDPR[9] guidelines. As a result, the platform was fined €310 million, issued a formal reprimand, and had its data practices overhauled

Online search

In 2017, insiders at an online search platform were revealed to have deliberately covered up a data breach that happened a few years prior. The breach exposed the private accounts of 3 billion of its users. Failure to inform stakeholders immediately that users' private information had been stolen was poor business communication. It showed a lack of urgency by the company to do right by their customers. By not addressing the crisis at the earliest opportunity, the company suffered a decrease in valuation, damage to brand reputation, and loss of employee and customer trust

[9] General Data Protection Regulation, the EU's information privacy regulation

Operational excellence + Business Resilience

Global telecommunications company

In 2024, a global telecommunications company's 5G network experienced a 12-hour-long outage. This cut off access to voice and data services for 290 million people across the United States. This included access to emergency services like 911 on the go.

Despite the scale and severity of the outage, employees of the telecommunications firm failed to acknowledge it until 7 hours later. They did not update customers on the disruption through WiFi calling. Unlike news outlets, they also failed to inform customers of alternative ways to access emergency services. Frustrated, customers took to social media to blast the firm's lack of communication and transparency. As shown, the employees' lack of adherence to recovery procedures and slow communication undermined customer trust



Compliance + Cybersecurity

Employees who fail to comply with industry regulations or company guidelines may harm their firms. With core corporate functions going digital, it is imperative for employees to keep pace with new digital protocols. The following example corroborates these points.

American retail mortgage originator

In 2019, an employee received a phishing email disguised as a business partner's message. Despite the email system being protected by multifactor authentication (MFA), the employee approved the hacker's MFA prompts four times before alerting IT. This was against the company's standard protocol, which required employees to:

- Recognise signs of phishing
- Question unsolicited MFA requests
- Provide timely escalation of suspected cyberattacks

Due to the employee's poor cyber hygiene, his email account, which contained sensitive customer financial data, was compromised. The retail mortgage firm was subsequently fined $1.5 million.

American big tech companies

Hackers targeted two American technology companies in an extended phishing campaign from 2013 to 2015. The attackers impersonated a Taiwan-based vendor for both firms. They sent a series of fake invoices to unsuspecting employees who "regularly conducted multimillion-dollar transactions" with the vendor. These employees wired funds to the fraudulent account without further verification. This was against the companies' cybersecurity guidelines, which required employees to recognise signs of phishing and authenticate large transactions.

As a result of the involved employees' noncompliance and lack of cyber hygiene, the two firms cumulatively lost $100 million.

Success Stories (Illustratives)

What does it look like if our Tech-enabled Workers have the necessary Digital Trust skills? Here are some illustrations of Digital Trust in action.

Digital Trust in HR when using data and AI

Tom is an HR practitioner at a local tech SME in Singapore. With the trend of accelerating digitalisation, Tom is increasingly finding himself having to analyse large chunks of company and employee data.

Tom has recently been assisting with the rollout of an AI project to understand employee engagement and attrition risks. Tom is not directly involved in the building and training of the AI algorithm. However, he knows after receiving basic digital trust training that he still plays a vital role in the ethical and responsible implementation of AI.

As such, Tom performs the following actions:

- Meticulously prepares the datasets for training of the AI model, mindful to exclude features that are demographically rooted like gender and ethnicity
- Personally vets the AI-suggested outputs with his fellow HR colleagues for fairness and accuracy
- Ensures clear and consistent communication between the project team and the company employees throughout the project lifecycle

Because of Tom's understanding of AI ethics and data analytics, he managed to:

- Mitigate bias in the AI model. As the model produced fair outcomes, it was readily accepted by employees. This promoted quicker rollout of the model, reaping productivity gains for the company.
- Avoid misusing biased data. In the sensitive circumstance of determining employee attrition, inadvertent usage of biased data may lead to discriminatory HR practices. Once uncovered, lawsuits, fines and reputational damage may follow.
- Enhance transparency and assure employees of the privacy of their personal identifiable data. This strengthens the culture of digital trust within his firm, facilitating future implementations of productivity-enhancing technological tools.

Digital Trust in Product Management to ensure cybersecurity and business resilience

Mr Low is a seasoned product manager who has worked in a number of tech SMEs. He believes that as a product manager, his job is about helping and understanding people—their needs, pain points, and desires. Therefore, he does what he can to ensure his customers get the best experience possible. As his tasks move online with digitalisation, Mr Low understands the need to pick up a few "digital trust" skills to uphold this commitment to his customers.

When planning for product launches, Mr Low leverages predictive analytics tools to forecast customer responses. In the process, he utilises data obtained from tracking customer behavior across various touchpoints like websites and emails. Mr Low ensures the following when handling customer's personal identifiable data:

- Consent is obtained from customers
- Purpose of how data will be used is properly communicated
- Data is promptly disposed of after use

Mr Low also goes to great lengths to safeguard customers' private information. He does this by practicing good cyber hygiene. This includes actions such as:

- Updating security software regularly
- Downloading endpoint protection software

Should disaster occur, Mr Low has built a set of protocols. Responsible for managing all aspects of in-life products, he will:

- Swiftly manage customer feedback and issues
- Provide clear and timely updates to affected customers
- Collaborate closely with internal stakeholders on the recovery plan

With the above guardrails and processes in place, Mr Low manages to achieve the following:

- Through transparent data practices, Mr Low fosters customer trust. This increases customer retention, thereby increasing revenue for his firm.
- Through practicing good cyber hygiene, Mr Low prevents malicious actors from illegally accessing customer data and disrupting his firm's critical business processes. This safeguards the privacy of his customers and ensures business continuity.
- Through timely execution of the business recovery plan, Mr Low reduces confusion among his customers and facilitates the quick resumption of normal operations. This reduces the extent of reputational and financial damage to his firm.

Digital Trust in customer relations to build business resilience

Jane is a fresh graduate whose first job is in customer relations and marketing. Her job scope comprises:

- Creating sales plans and marketing strategies
- Building relationships with existing and potential customers
- Identifying sales and marketing opportunities

With rapid digitalisation embedding technology into her core work, Jane understands that "operational excellence" now goes beyond proficiency in her main tasks. It now includes:

- Leveraging technology appropriately to improve productivity
- Dealing with fallout caused by technological failure

With this in mind, Jane is extra mindful when utilising AI tools — be it for improved lead management and targeting, behavior tracking or customer insights. Being ever-vigilant of AI hallucinations and bias, she:

- Engages in thorough cross-checking of AI recommendations for transparency and fairness
- Evaluates applicability of all AI-generated advice with her team before implementation

Her due diligence proved pivotal when she blocked an AI-generated marketing campaign containing falsified statistics, averting a possible public relations crisis.

In addition, Jane deftly executed the business recovery plan following a large-scale, nationwide IT crash. Being conversant with her company's standard operating procedures, she immediately performed the following actions:

- Pre-empted and managed customer queries regarding the disruption
- Provided timely and consistent updates of the situation to customers

Her actions drew praise from customers. They maintained that her prompt, proactive and transparent communication reduced confusion and assuaged their concerns. This helped Jane’s company stand out amidst the competition which faced the same outage.

Digital Trust in compliance, with cybersecurity

John works as a financial accountant in a local tech SME. His job scope requires him to:

- Compile financial statements
- Report on the company's financial health and liquidity
- Audit financial transactions and documents
- Ensure compliance with financial policies and regulation

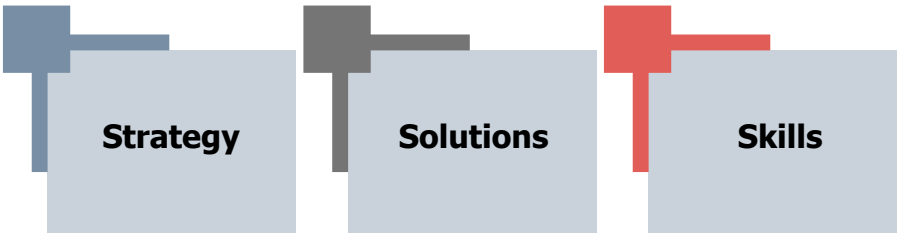
Due to the confidential and sensitive financial information he handles, John is a prime target for cyberattacks. Aware of this, he complies with his firm's cybersecurity protocols to protect against threats, which includes:

- Installing security tools
- Downloading anti-virus software
- Having strong passwords which are regularly updated
- Using authorised devices
- Prohibiting unauthorised software downloads
- Recognising illegitimate emails and signs of phishing

John's commitment to practicing good cyber hygiene reduces the likelihood of a successful cyberattack on his company. This decreases risk of possible litigation, reputational damage and disruption to services.

7 CALL TO ACTION FOR SMES

The findings of this report make it very clear that all companies, including SMEs, need to urgently equip their workforce with Digital Trust skills as part of their digitalisation journey. Fortunately, there are many forms of support available to companies that want to digitalise - at the level of Strategy, Solutions and Skills.



For companies that are just embarking on their digitalisation journey, programs such as SGTEch's DT-SME are designed specifically to equip SMEs with the essential tools and **Strategies** required to excel in the digital age. SMEs can also leverage SGTech's curated pool of **Solutions** that are tailored for SME use cases.

For companies that have already embarked on digitalisation, the immediate focus should be on building Digital Trust **Skills** in their Tech-enabled Workers. While there has been significant upskilling of staff, these have often focused on enabling them to use the new technologies effectively. SMEs need to recognise that Digital Trust skills have become an integral component of many job roles, even those that are not traditionally thought of as "tech roles". They need to identify the Digital Trust skill gaps in their current job descriptions, and update their JDs accordingly.

The critical step is to ensure that current (and future) employees are equipped with the necessary skills. This can be through a combination of on-the-job training and external courses, leveraging the funding available for upskilling. SMEs can tap skills programs such as Career Conversion Programs (CCP) to provide their teams with the training and learning they need to build Digital Trust skills. Companies can also use other forms of support such as SkillsFuture Enterprise Credits (SFEC) to fund the journey as they build Digital Trust skills in all their Tech-enabled Workers.

Training providers have the challenging task of translating Digital Trust skill needs into compelling training programs. The programs must be tuned to the needs of different groups of Tech-enabled Workers with different levels of technical proficiency. Some of the Digital Trust skills identified in this report are already part of the national skills framework, while others have been modified. There would be value in curating new courses which bring together the disparate elements under one umbrella. Training providers should leverage existing resources and benchmarks, such as:

Skills Future Framework for the ICT sector

Data Protection Trust mark

Cyber Trust mark

Digital Trust skill definition

Knowledge & Abilities

Term	Definition
Artificial Intelligence	Responsible AI Framework (Fairness, Explainability, Robustness, Transparency, Data Privacy) based on IBM's Five Pillars of Responsible AI Adoption Ensure that responsible AI principles are upheld throughout the following activities: <u>Input</u> • Confirm that input dataset is accurate, representative, and meets the **data privacy** standards • Maximise likelihood of **fair** and accurate results by entering the right prompts <u>Processing</u> • When collaborating with AI development team to train models, ensure training data is **fair**, i.e., accurate and representative • Provide **transparency** by being able to explain it to stakeholders <u>Output</u> • Verify output for violations of **fairness** • Verify whether output violates **privacy** and confidentiality of personal/ company data • Assess the credibility and accuracy of information generated <u>Actions Taken</u> • Check that actions taken based on AI output are **fair** • Raise concerns to tech/development teams to maintain **transparency** • Sense-make and decide on whether to heed AI-generated advice based on individual context

Term	Definition
Business Resilience	Prevention • Adapt and adhere to company's newest standard operating procedures • Participate in tabletop exercises to help management identify points of failure in the overall operational resilience strategy • Deploy processes to manage technology implementation Detection • Recognise symptoms of failure • Practice rapid and timely reporting to the relevant management team for activation of whole-of-enterprise response plan Response • Communicate to external stakeholders (regulators, customers, investors) • Execute company's business continuity and crisis management plan
Cybersecurity	Prevent • Develop strategies to mitigate cyber security risks • Be familiar with organisation's IT policies • Understand types of cyber security risks • Conform to organisation's policies to monitor cyber security risks • Follow organisation's cyber security policies to identify potential risks Detect/Contain • Develop strategies to manage cyber security risks • Review usage of digital technology tools, systems and software to identify any breaches of organisation's digital and IT policies • Take preventive measures within power to ensure breach does not spread further

Term	Definition
Data Protection	Data Classification • Understand types of data and degree of sensitivity • Sort data by type and level of sensitivity to decide on appropriate protection measures Data Ethics • Understand Data Ethics Framework (Ownership, Transparency, Privacy, Intention, Outcomes) • Ensure that data is collected, stored and used ethically Data Protection • Develop Methods to safeguard data • Ensure physical safeguarding of data Data Regulation • Understand relevant Data Regulations • Be familiar with organisation's personal data and privacy policies • Ensure compliance with specific regulations for various types of data • Adhere to organisation's personal data and privacy policies
Emerging Threats	Lifelong Learning • Focus on adaptability and continual learning in fast-changing workplace Resilience • Build capacity to tide over challenges given fast-changing nature of work