

Digital Trust Reconceptualized in New Digital Technology Environment

Keyong Monty Guo

INSTITUT SUPERIEUR DES SCIENCES, TECHNIQUES ET ECONOMIE
COMMERCIALES

12, rue Alexandre Parodi - 75010 PARIS – FRANCE

khw753@outlook.com

Digital Trust Reconceptualized in New Digital Technology Environment

Abstract

Challenge modals imposed by new technologies has made human vulnerabilities the weakest link in digital trust practice. Previous research fell short in navigating the complexities of dynamic digital business contexts, based on digital trust theory and social-technical system theory, this paper investigated whether a preventive and dynamic comprehensive management system could deliver digital trust. It was conducted using an action research methodology. The outcome demonstrated subject organization has increased customer loyalty, reduced security issues, and met regulatory requirements, this outcome facilitated their digital transformation. This paper joins scholarly conversation on digital trust by including six new constructs, by reconceptualizing the theoretical framework in workplace into a vertical hierarchy structure framework typical of proactive and iterative features, and highlighted the roles of people' subjective initiatives and culture. It also provides insights to organizations for how to earn and deliver digital trust new normal in organization routines.

Paper Submission Type

Completed Research Full Paper

Track

e-Business and Information Systems Management Track

Word Count

Full Paper 5735

Key Words

Digital Trust, Hierarchy Structured Integrated Framework, Digital Ecosystem, Digital Resilience, Risk Audit

Introduction

The widespread application of AI in business, the gradual formation of the metaverse industry chain have brought more privacy and security risks and presented complex ethical and legal challenges. It has become an urgent task for us to build a new type of digital trust relationship and encompass user experience, data security, and legal challenges, including intellectual property rights and regulations in the context of AI and the Metaverse. In practical world, companies like Google, Meta and Microsoft had proposed “Zero trust”. Professional associations and non-profit organizations had also joined this effort by issuing AI ethics declarations. In the academic world most research had yet been focused on technology, some scholars had made research attempts from a process perspective, especially from IT-related data processing processes, hardware and software equipment, and people. But trust concerns were different, and so trust pattern should not be the same. From a user point of view, it didn't help much how to establish digital trust management in a trust-aware organization routine setting. An articulation of trust-aware process design through empirical investigation in the tradition of action research could have led to an iterative, empirically grounded development of the model (Rosemann, M., 2019).

To fill this gap, I posed the following research questions: 1. Could we instil in organization routines a hierarchically structured framework of proactive and dynamic nature by vertically integrating humans, technology, and process? 2. Could we mobilise people’s subjective initiative by centring and stakeholding them? 3. Do we need to expand digital trust to include the challenges posed by new digital technologies (United Nations. 2018; UN Secretary-General High-Level Panel. 2018; European Parliament. 2023)? These questions are important because facing increasingly complex and severe network and information security situations, such as frequent data leaks, frequent network attacks, espionage etc., how to prevent and control information security risks and ensure the security of key information assets in digital transformation is an urgent problem to be solved. With the goal of the orderly operation, problematized problems must be focused on how to improve the institutional arrangement and relationship coordination mechanism, and gradually improve the information security governance mechanism from different dimensions such as compliance, contract, relationship, and process.

The purpose of the study was to capture perceptions and practices of digitally transformed organization’ leaders and develop an understanding how they addressed key challenges by conducting action research in ‘how’ they perceived and practised a range of operational and strategic initiatives to responsibly resolve those challenges. A framework was developed to understand ‘how’ their initiative had been implemented in daily operational scenario, the strategic, their conceptualised and practicalised understanding. In the study the author defined digital trust as to trust in data, information, transactions, and interactions in a digital world. It was trust built on a safe, secure, and available, ethical digital environment.

This paper is structured as follows. Section 2 literature review: digital trust concept evolvement and research question. Section 3 elaborates research methodology. Section 4 is the findings. Section 5 discussion: what the elevated meaning my research will be in relation to background

and research framework. Section 6 conclusions: what my contribution is to the knowledge body of digital trust, what the limitations, and practical implications are.

Literature Review

Digital Trust Theory

With its research across heterogeneous domains such as psychology, sociology, philosophy, and economics, definitions of digital trust were difficult to substantiate to a single one (Corritore, C.L et al., 2003). The most quoted one is digital trust "underpins every digital interaction by measuring and quantifying the expectation that an entity is who or what it claims to be and that it will behave in an expected manner" from Gartner Inc. (Marcial, D.E et al., 2022). The review in this study shall divide it into technical means, perception and behaviour, control and surveillance, model or process etc. four categories.

Trusted Computing Technology

In various digital environment, there is need to security guarantee, privacy protection, prevention of offences and exceeding statutory scope government surveillance, data and digital assets protection. With the advent of new digital paradigm, scenario adaptable computing technology has been adopted to deliver trust. To ensure security, privacy and trust evaluation mainly in mobile platforms, cloud computing and cyber-physical systems, an extended Trusted Platform Module created in 2014 by Akram, R.N., & Ko, R.K. With remote work and collaboration increased sharply, and cloud-based assets were not located within company's premises, a zero tolerance architecture had been articulated by Rose, S et al (2019). For handling privacy issues in among the IoT devices, TURP, a technique was perfected by Kökciyan, N., Yolum, P. (2020) using a disjunctive logic programming language. With ever severe illegal behaviours, cybercrimes and state surveillance were hampering trust and confidence on line, a network architecture that generates trust in transactions by a trusted third-party system, blockchain has emerged (Isaac, H., 2021).

Cognition, Perception, Emotions, Behaviours and Social Motives

The earliest typology of digital trust was made by McKnight, D.H et al (2001). Digital trust were expressed by concepts of cognition, perception, behaviours, motives etc. which were borrowed from psychology, sociology and social psychology. At first, it meant security risks and trustworthiness on internet components of merchant, shopping medium, contextual infrastructure and other factors (Matthew K. O. et al, 2001). Corritore, C.L. et al (2003) extended to include other perceptual factors: credibility, ease of use. By degree, an e-vendor's social presence of integrity, predictability, ability, benevolence in b2c(business to customer) e-commerce environment (Gefen, D. and D. W. Straub, 2004; Hawlitschek, F. et al, 2016), user perception, user satisfaction, user expectation (Beldad, A. et al, 2012), social motives (Mittendorf, C., and Ostermann, U., 2017) were added. Yuanyuan Guo (2022) defined it as cognitive trust mixed with emotional trust. Cognitive trust were measured by practicality, commitment to execution, honesty, benevolence, while emotional trust included likes, beliefs. Finally, organization's reputation, business partners' reputation, customers' privacy, business partners' risk, regulatory authorities' regulatory oversight were all important security concerns in building trust (Barbara

Wyrzykowska, 2020), for they would be involved. In as early as 2011, Buechner, Jeff et al established a trust model of digital agents, into which they incorporated self-trust of human agents and artificial agents. When artificial intelligence has entered a new epoch and replaced more posts occupied by human beings, a new kind of trust has been put to the centre. Contrary to Buechner, Jeff et al, Ryan, M. in 2020 claimed AI was not something as trustworthiness, for it does not possess emotive states or can be held responsible for their actions.

Control and Surveillance

In the context of P2P (purchase to pay) collaborative consumption platforms, trust building were measured by reliable insurance cover, simultaneous reviews, and worldwide large network. If platform provider had been trusted, it was highly probable that merchant peers would get trusted too (Möhlmann, M., 2016). If the goal was for control and surveillance, in order to regulate data usage and prevent privacy intrusiveness, policies and activities needed to build into business model, this would be a good mechanism to realise (Cecere, G. et al, 2013).

Process Model Management

In collaboration with their global partner, Marcial, D.E. et al (2019) launched a global-wide study of digital trust in the workplace with an emphasis on people, technology, and process. An Input-Process-Output model were formulated. The core of this framework was management. The results indicated that level of priority, experience, behaviour and attitude were the main reasons that impact trust. Rosemann, M.(2019) created a meta model for Trust-Aware Process Design. He argued uncertainty, vulnerability and confidence were the core elements of trust and organizations need to identify moments of trust, reduce process uncertainty and reduce vulnerability. Later on Müller, M.P. et al (2020). applied a bottom-up approach to identify what were and where the uncertainty was and they revised earlier trust model for business processes (TRUB), their contribution was an analytical way to visualize the uncertainties.

Socio-Technical Theory and Digital Trust Management

The social-technical theory developed by analytical empirically-based researchers to study IT and social change, and it had become the major underpinning of efforts involving work design (Kling and Lamb, 1999; Peter M. Bednar & Christine Welch, 2017). When talking about trust management, we need to focus on peoples, according to a philosophy of human-centred design and by taking into account systemic interactions among peoples and technologies.

Summary, Critique and Research Framework

The connotations of digital trust in previous research gradually shifted from psychological, societal, behavioural factor to objective factors. Mattila, J., & Seppälä, T. in 2016 argued digital trust could be built on a combination of three factors of security, identifiability and traceability. Barry Connolly (2020) added transparency and interaction. In this research I defined digital trust as to trust in data, information, transactions, and interactions in a digital world (Jim Boehm, Liz Grennan, Alex Singla, Kate Smaje, 2022). It was trust built on a safe, secure, and available, ethical digital environment. It could be measured by measurements such as data availability for raising productivity and innovation, data trustworthy and quality, data protection and confidentiality, data governance and AI for IoT ethics, digital supply chain safety, information systems resilience and business continuity (The World Economic Forum. 2022; Global Digital Trust Insights. 2024; Ejjami, R. 2024; Sarno, & Maulidar.2024).

Past research indicates that technology alone can't build long-term trust. "Control and Surveillance" was the first step in the academic community, the next step was management of IT process. The problems that enterprises are facing now is changing with the continuous advancement of technology. The previous research on digital trust is macroscopic, and it is not of much help to organizations to earn digital trust. Take the latest research by Launer, M. et al for example, They limit the level of digital trust in people to IT equipment and its users, and only studied data protection and process handling data (Launer, M., Svenson, F., Ohler, D., Meyer, J., 2020). A comprehensive approach to examining digital trust, which encompassed management (Barbara Wyrzykowska, 2020), new digital trust needs, skill acquisition (Marcial, D.E., Arcelo, A.Q., Montemayor, J.O., & Launer, M.A., 2022) have been put on the agenda (Launer, M., Svenson, F., Ohler, D., Meyer, J., 2020). What we urgently need to do in the digital era were to protect our data and ensure our organization be compliant with regulations and requirements, to establish an open policy of cybersecurity strategy to protect our organization against breaches and attacks, and to understand and mitigate risk in our digital supply chain and maintain a relationships in a controlled and secure manner. Ideally employee have to play a more important role.

I followed the direction pioneered by Marcial, D.E., Arcelo, A.Q., Montemayor, J.O., & Launer, M.A. in 2022, I formulated a hierarchically structured framework that integrated people, technology and organization routine business process. In contrast to theirs, I build this framework vertically into 3 layers. The basic layer is a technological gateway (Isaac, H. 2021), which will block most unwanted, and incompliance visit or intrusion. The middle layer is people. Those personnel who manages, runs, programs, and maintains an information system can affect digital trust building in an organization (Marcial, D.E., Arcelo, A.Q., Montemayor, J.O., & Launer, M.A., 2022). Workforce differentiation consists of identifying then motivating high-performance employees and ensuring that they take the strategically critical job positions. "Employees are more likely to be rewarded for generating new ideas, taking appropriate risks, and following test and-learn practices as they pursue opportunities" (Mc Kinsey, 2019, p. 4). Through empowerment and motivation process, all the people in the organization shall get engaged. Trust awareness, digital culture are most important in the layer. The topmost layer is a management system of sequenced and interacted business processes. Digital technologies will undeniably bring about great changes to organizational business process, even business model, thus it implied the management style change of business processes (Renner-Micah, Anthony; Effah, John; and Boateng, Richard, 2023). Research demonstrated that a holistic strategy to address cybersecurity and deploy best practices would help organizations in their digital transformation initiatives (S. Mishra and S. Gochhait, 2023). Client requirements and legal compliance are catalyst for business growth. An improvement mechanism of risk audit, management review, and third-party certification are to perfect the system.

The following is the hierarchically-structured management system integrated people, technology and process (refer to Diagram 1. Hierarchically Structured Integrated Framework).

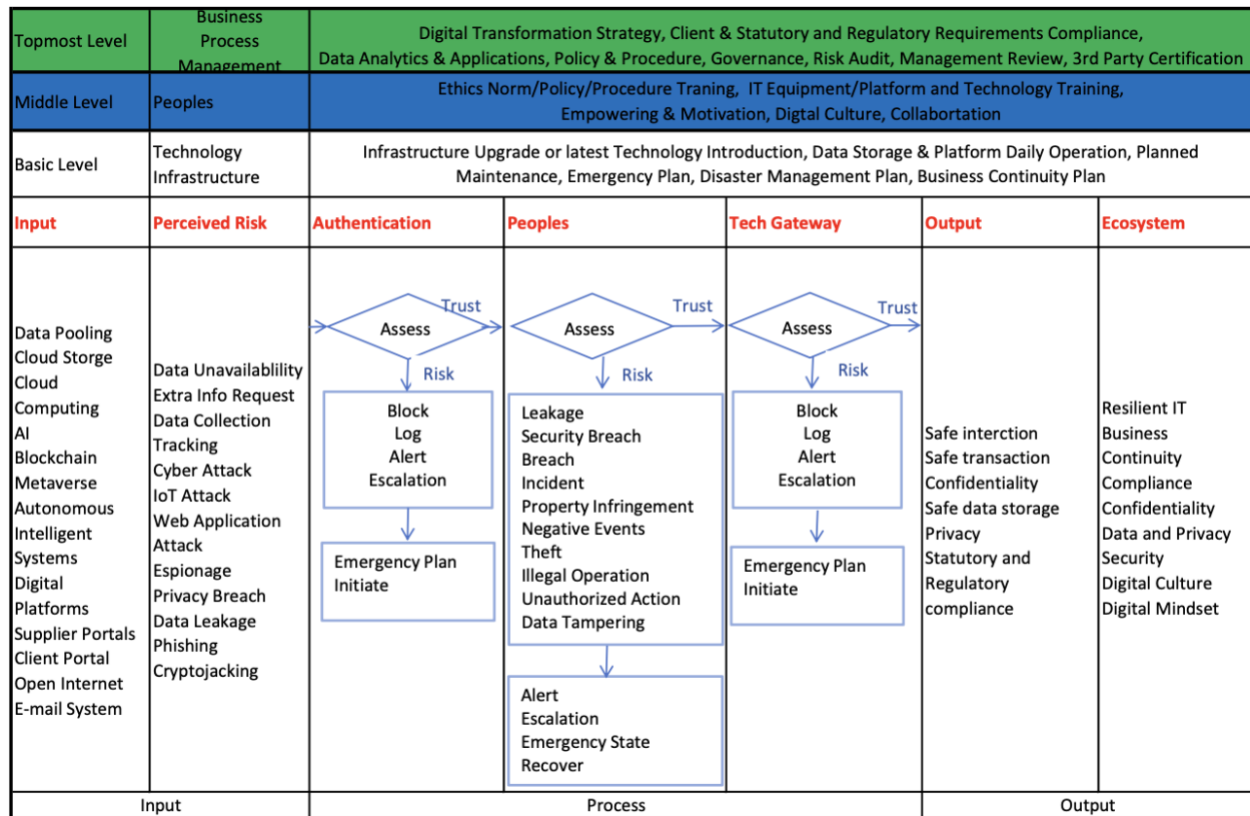


Diagram 1: Hierarchically Structured Integrated Framework

Methodology

New Technology environment in this paper has been defined as data pooling, AI-driven analytics, cloud computing, Internet of Things (IoT) devices, artificial intelligence (AI), blockchain, metaverse, Autonomous intelligent systems (OECD Secretariat, 2019; Sarno, & Maulidar 2024).

This study was conducted using action research study methodology. Action research begins with the experience of an organisational problematic issues and change orientations, then to introduce new changed practices in social contexts and involves other people, and monitors the results, the research requires active co-operation between researcher and client and a continual process of adjustment to the intervention in the light of new information and responses to it from respondents, this process often shows cycles of action and reflection.

The subject organization was a Chinese Printed Circuit Board (PCB) manufacture. It had around 1,000 employees and it had passed level 5 of China's Intelligent Manufacturing Maturity Model assessment. There were several reasons for the selection. Being an intelligent manufacture, into a B2B (business to business) platform it had integrated suppliers, subcontractors and service providers, and client manufacturer, trade firms. Except for ERP, MES and OA, AI had been used in IoT system of AGV, Andon, MES, RFID, as well as wire pattern and cosmetic appearance

inspection. They had encountered all the problems data stewardship, cybersecurity, and privacy breach. It was very suitable for my enquiry purpose. The study was to track the changes made in the organization in a scientific and objective way of digital trust management in their digital transformation process.

The potential benefits lie with the powers of reflective thought, discussion, decision and action by organizational actors. Pitfalls and challenges inherited with the method would be participation, the role of reflection, the need for knowledge management, and the ethics of the process. In order to address these concerns, the research team consisted of two members, the author and the other, a veteran researcher with PCB expertise, he had been recruited from a multi-disciplinary study perspective. The research team had specific roles, sometimes performed independent investigation tasks, shared a common goal and a procedure how to act and work together. Before project, the author had signed an agreement with the subject, in which the scope boundary, mutual responsibilities including conflicts and continentality, attention points, the use of research results, and entry and exit requirements had been defined. This research carried out from July 2021 to July 2023. The study conducted in three phases of data collection, encapsulating the five steps of diagnosing, action planning, action taking, evaluation, and specifying learnings as follows.

Diagnosing

By interview, observations and records retrieval, the researchers conducted one-week process approach diagnosing audit. Disasters, emergencies incidents and negative events, together with its information system infrastructure, digital applications and its management system had been assessed. Organizational problems were required to show not through reduction and simplification, but rather in a holistic fashion. The outcome was used to develop theoretical framework.

Action Planning

Together with the management team, applications end-users, clients and suppliers as appropriate, the researchers discussed an action plan, which was guided by the theoretical framework indicated both some desired future state and the ideal change state. Target of phases and timing plans were initiated.

Driving Change, Action Taking

Approaches were mainly observation, interview and focus group. Actors involved were CEO, CIO, user department managers and engineers. When lagged behind the schedule and not hit the target, “directive” or “directs” intervention tactics were adopted to ensure expected changes to be made.

Theoretical Effects, Evaluating

The collaborative outcomes had been evaluated. The researchers and organization actors together assessed whether the theoretical effects of the action were realized, and whether the problems had been solved because of these effects. Where the change was successful, it must be critically discerned whether it was the actions taken that were the sole cause of success. Where it was unsuccessful, another cycle of action research (including adjusting the hypotheses) were taken.

Specifying Learning

The process for specifying learning had been taken iteratively. The knowledge gained in the action research were used to restructure organizational norms by top management teams, to provides important knowledge to the scientific community for dealing with future research settings.

Data Collection

For data credibility and validity, data analysis had been an iterative processes together with multi perspective triangulation. In the course of the research, the researchers participated in 12 seminars and interviewed 3 top, 8 managers and 12 staffs successively. In addition, The researchers had access to organization's internal and archival documents. To observe the changes taken place, the researchers also participated in the management team's planning and decision-making meetings.

Data Analysis

Beginning from the 2nd phase, the researchers interacted with and made sense of what had gathered in data archive, such as diaries, memos, questionnaires, audio-recorded comments, pictures, field notes, email exchanges and meeting minutes. We established themes, ideas, concepts, keywords as our coding criteria, that's also called thematic analysis and looked thoroughly for it in these data or text.

To show the internal authenticity of the data, the researchers team made ensure that it has some kind of authorisation from the data source, such as signature on a photograph, a time and date on a video or a mark of confirmation of ownership, the manufacturer's logo etc. Data analysing was conducted from both a surface-level factual perspective and also a deep-level meaning-making perspective (Jean McNiff, 2017).

The authenticity of the data then needs to be approved and agreed first by the co-author and then by organizational participants and got their critical feedback. We also used triangulation in data gathering, analysis and interpretation (Yin, 2016), comparing with theories in the literature, to show how we were agreeing with them, developing them or challenging them.

Findings

Technology Infrastructure, Operation and Maintenance Management

To prevent attacks across web, application, content, and devices, the organization introduced an ASIC-based firewall that uses a combination of signature-based and behaviour-based technologies to analyse network traffic for signs of suspicious or malicious activity, and in the event of a malicious network, the firewall with pre-set security alerts would immediately send an email or SMS Notify the administrator/operator to generate an SNMP trap to be directed to the network/asset management application.

In order to ensure IT service disruptions are dealt with quickly, that normal service operations are restored, and that potential damage to business processes is prevented. IT specialists and platform administrator swiftly identified, analysed, resolved incidents to minimize their impact, and escalated problems when necessary. To prevent the recurrence of such incidents, they would periodically maintain all systems and regularly update their software and operating systems, while conducting regular and frequent security audits.

When a network infiltration unfortunately occurs, how could the organization use technology gateway to deal with disasters? A Network Intrusion Detection System (NIDS) with neural network, artificial intelligence capabilities would monitor network traffic and upon discovery of an attack, alert security personnel and impacted users and clients. A Network Intrusion Prevention System (NIPS) functions more like a stateful firewall and would automatically drop packets upon discovery of an attack, initiate actions to block suspicious traffic or reroute it to a quarantine environment for further analysis. Under severe conditions, the technologies would disable network connectivity, disconnect compromised devices, or implement network segmentation to create separate network zones to limit the attack's spread. After all that, firewalls would be configured to block future attacks.

Proactive and Dynamic Comprehensive Management System

To build digital trust, an organization needs to take ownership of their cybersecurity transformation, enabling them to quickly identify, mitigate security risks, and ensure compliance and being ethical. System transformation emphasizes the transformation of personnel, organization structure, culture and integration with other management systems. Top management team should ensure organizational data strategy and policies are implemented in the system. The establishment of digital trust management system for subject organization were divided into two phases. The first was process mapping and documentation. A team was assembled. After thorough diagnosis, the team set out process mapping. The team found except a few, the rest processes did not need to be re-designed. When designing a process, key digital risks, stakeholders and legal requirements compliance restrictions were identified as input. Then security and error-proofing technology were defined. Next, owners and risk responsibilities were assigned. Finally, key efficient and effective metrics were set up, risk prevention instructions and control procedures were prepared. As output, expected ideal cyber state was made clear. Emergency plan and escalation process were prepared in critical digital processes, when anything could not go as expected, escalated response plan would be initiated. Later in the phase, the team began to write documents, design report and record format. The second phase started with documentation release, then training and testing were done. Two months later auditors were trained and an internal risk audit were conducted to assess conformity and compliance status. If any non-conformances were raised, action plan was needed to rectify. The findings and follow up were reported to top management team.

The subject organization established a hierarchically-structured comprehensive management system, into which integrated people, technology and process. The basic layer was technological infrastructure, it could guarantee ongoing operation by built-in technology. The middle layer was people. If someone did not abide by norms, procedures and policies, an alert should be sent to process owner, and IT administrator concurrently. Required containments actions commensurate

with its severity should be executed. If not ineffective, company-level disaster management plans would be activated in accordance with the escalation process. The information security risks in the organization was normally monitored by IT centre and process owner, the reporting line were CIO and CEO.

Digital Resilience

How could digital trust management system become resilient? First, it must be flexible and enable organization to respond quickly and effectively to various business disruption events. Business recovery plans would be aligned with disaster management plans, business continuity plans. Next, organizations must adopt a "total disaster" approach when identifying potential sources of business disruption, including gathering threat intelligence information and acting on identified threats to remain resilient to cybersecurity risks. Resilience must consider the ability of a business to remain operational in the face of multiple risks. Organizations should consider supply chain risks and integrate with customers where needed and possible. To adopt a preventive and predictive approach was extremely important.

Centring and Stakeholding Peoples

All employees were involved and digitally competent. All employees, especially those in charge of AI, and in key business units, were oriented, and trained on cybersecurity threat awareness, how to use AI and intelligent devices. When people were trained correctly, they acted as multipliers in their departments. They could fulfil their duties by not imposing any risks and causing negative events. Then, the organization could ensure through ethical behaviour and sound governance that it can protect, store, and secure the data in its care.

In order to have a clear understanding of people management and how important roles they played. The researchers conducted documentation review. It was seen that IT governance structure, principles and policies, ethics norms had been posted in digital key areas. IT requirements had been clearly defined in job descriptions of B2B (business to business) platform chief administrator, low-code programming engineer, ERP and MES supervisors. Disaster recovery plan, internet hacking emergency plan, incidents reporting line and handling procedure had been reviewed. In one tour to Marketing & Sales Centre, one staff just returned back to work seat, when talking about client specific requirements, "We have assigned confidentiality contract with our company, even if minutes away from computer, we have to lock the screen in case unauthorized log in not happen. We are forbidden to transfer clients data and transaction documents through unqualified social media channels or Apps," She told us. Another time in a B2B platform penetration drill, it had been observed that the CIO assumed commanding authority, key department managers participated. A major incompliance had been raised and reported to the General Manager, for an obsolete encryption protocol had been used due to the engineer in charge being away on holidays the backup engineer forget to update. The researchers also revised the action plan.

Knowledge and skill training programs must be relevant. Training in subject organization consisted of three types. The first was orientation, main contents were security threats awareness, norms, principles and policy, client specific requirements. The second type, TWI (training within industry) composed of knowledge and skills. Specific technical instructions, and work flow &

procedures, job relations were trained and qualified before assumed job positions. The third type, OJD (on job development) was conducted according to yearly training program. It covered all employees, new products & service, organization manual and procedures, introduction of AI, Metaverse and big data, ISO27002-2 and IEEE standards. Due to COVID 19, except TWI, all other types of training had been performed online. Most-commonly used forms were workshops, seminars, media education courses. CIO was observed to be in charge of intelligent manufacturing, digital technologies.

The subject organization had unique digital culture. Employees had to be empowered through technology that makes it easy for them to do the right thing and hard for them to do the wrong thing. As key 'trust stakeholders' for their products and customers, they were not just following orders from a IT centre but rather were following the rules because that was what their customers expect. IT and cybersecurity teams should actively engage with other departments. By understanding their security concerns and emphasizing the significance of cybersecurity, these departments can bridge gaps and work in tandem. By working together, they can leverage shared knowledge, resources, and expertise to enhance threat detection, improve incident response, and strengthen their overall security posture. CEO was observed to coordinate the work of IT, Production, and Marketing & Sales in the course of AI introduction and MES update in order to ensure these functions to comply with the new regulations. Focus group interview was conducted to get the employee's perception of digital trust program. Participants mentioned that digital trust had already been a culture in their company, that they could earn trust from business stakeholders and at the same time deliver trust to them. "Our company want to become a leader in China's PCB industry. So we have to be digitally resilient. In order to compete, we have to build a business ecosystem," added the Assistant General Manager.

Leadership and Commitment

Involvement of top management and board was critical to organizational success. Employees must be responsible to CEO and in return CEO must be responsible to stakeholder board. CEO in subject organization developed a three-year business plan, with smart manufacturing and digital trust in it. He communicated to management team through monthly operational meeting, to all employees through quarterly employee briefing. He was also observed to publish restructured organization chart, to make arrangement to hire data analytics engineers, iCloud engineers and AI engineers. He chaired the investment meeting of AI and MES update. He approved norms, principles and policy, company-level procedures, disaster recovery plan, escalation process. Risk audit had been performed in line with internal audit program supervised by CIO. Audit report and action plan would be reported to CEO for review.

Extended Digital Trust Constructs

The subject organization had invested successively AI in marketing process, MES scheduling process, and wire pattern, cosmetic inspection process. In solder paste injection and pattern developing process, augmented reality technology were introduced. All data from local servers were transferred to Alibaba iCloud. Only organizational level control of email phishing, internet hacking and ransomware were not enough. What challenges it would be? The researchers attended their management meetings and also interviewed top management and managers. The interviewees told us that in their minds they had already designed how to include data leakage and security in iCloud and B2B platform, privacy intrusion and incompliance incidents on both

internal and external systems. “We had already colossal of data, and initiated a program to make best use of it by using data analytics. In order to safeguard our business achievements we had to create a digital ecosystem by integrate our subcontractors, suppliers, even our customers into the system. At present, we could not afford to lose fame and revenue, we had to build a resilient digital system,” the CEO stated. When we interpreted these findings, we could see they changed their mindset. In new technological environment, digital trust had new features. At least data availability, data worthiness, data protection and compliance, AI for IoT ethics had to be encompassed to deliver a comprehensive dynamics.

Discussion

By exploring how engagement of employee influence digital trust managements outcome. The study contributed important theoretical insights to scholarly discourse focusing on digital training, motivation, and culture. It helps to illuminate its significance in countering dysfunction development and fragile sense of security. To those persons affect legal requirements, data leakage, privacy breaches and theft of intellectual property, training programs for them shall be prepared and updated in line with technological advances. Organization also needs to empower people through technology that makes it easy for them to do the right thing and hard for them to do the wrong thing. Organization creates a culture of openness and transparency will find it easier to build confidence in products and solutions that embrace a digital world. Previous research showed that one person or department in charge of IT technologies should guide and train the employee according to their job risk effects. On the other hand, all effort should be exerted to raise trust perception (Marcial, D.E., & Launer, M.A. 2019; Marcial, D.E., Arcelo, A.Q., Montemayor, J.O., & Launer, M.A., 2022).

The author investigated how can a re-structured comprehensive management system could address new modal challenge. Through the extension and reconceptualization of the framework integrated people, technology, and process. The author was able to show how a preventive and predictive mechanism manifest routine control and surveillance across three vertical layers. This framework then allows the author to examine organizations could provide trust to the relevant stakeholders as well as actively prevent and predict potential risks. These proactive measures should be dynamically adjusted according to any changes in business processes. The top management should propose and develop a security strategy that focuses on digital governance and the use of data analysis techniques and data applications. They shall make installed an internal control mechanism that is capable of self-improvement by risk audit and managerial reviews. Organization should understand and mitigate risk in their digital supply chain and maintain a relationship in a controlled and secure manner. ISO/IEC27002, ISO38505, ISO27701 third party certification, new technologies testing are conducive to the structured and disciplinary management. Due to variant technologies and personnel IT literacy, previous models could not help organizations to implement digital trust. Their perspective was not from company’s wide angle but from that of people or equipment for information processing.

With this study, we gave new meanings to digital trust. In previous studies, all measurements were defined from cognition, perception, behaviours, emotions, and social motives etc information processing processes in psychology and behaviour science. Due to the advent of

Web 3.0, Industrial 5.0, AI and Metaverse technologies and the complexity of cybersecurity has been doubled, Data availability, data trustworthy and quality, data protection and confidentiality, data governance and AI for IoT ethics, digital supply chain safety, information systems resilience and business continuity have been singled out conspicuously.

Conclusions

Data security and frequent internet negative events provide great challenges never met before, with more and more organizations initiated digital transformation programs, and the rapid development of digital economy, which powered by AI and metaverse. Building and delivering trust in digital environment is even more important, and it can both boost the prosperous development or destroy an organization. My research demonstrated that risk can be mitigated, business affecting negative events can be avoided. Since trust groundwork has been laid for seamless interactions and transactions, routine operation remains secure, and business will be unlikely to be interrupted that easily.

This study contributed to the digital trust literature in three aspects. First, I added to the model new components such as culture, value and strategy, and coined new measurements in evaluating digital trust outcome. Next, I restructured people, technology, and business process vertically comprehensive management system. The framework is technology-based, digitally human-centric, and emphasizes proactive prevention rather than reactive response, and is integrated into the day-to-day operations. Finally, I enriched and concretized digital training. From action research lens, I contributed to new practices by showing how people can change their own situations. I had also contributed to my theoretical framework by showing improvement in my own thinking and have deepened insights around my research issue.

However, there is still limitation in the research. This model has been tested only in digitally transformed manufacturing organization. The future re-test research in digital economy platforms, service industrial sector and e-governments are encouraged.

The contribution to organizations and practitioners would be lessons learned that can be put to use. Organization shall embed privacy and data protection at the heart of the organization's culture and operations. It is not very effective to only control in a pre-set isolated scenario, and it must be controlled by the whole business process of the whole company. Technology assurance is the foundation. Upon which was a comprehensive system that proactively reduce and respond resiliently to cyber threats. It is security-minded people that ensure operations are not adversely affected through daily management.

References

Akram, R.N., & Ko, R.K. 2014. "Digital Trust - Trusted Computing and Beyond: A Position Paper," IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, pp.884-892. <https://doi.org/10.1109/trustcom.2014.116>.

Barbara Wyrzykowska, 2020, Digital trust in business and society in 2020 digital trust conference proceedings 4. Service Management Congress Digital Trust & Intuition @ the Workplace.

Barbara Wyrzykowska. 2020. "Digital trust in business and society," in Digital Trust & Intuition at the Workplace Conference Proceeding of the 4th international Service Management Congress, Ostfalia University, Suderburg.

Beldad, A., van der Geest, T., de Jong, M., Steehouder, M. 2012. "A cue or two and I'll trust you: Determinants of trust in government organizations in terms of their processing and usage of citizens' personal information disclosed online," *Government Information Quarterly*, (29:1), pp. 41–49. <https://doi:10.1016/j.giq.2011.05.003>.

Bednar, P. M., Welch, C., Milner, C. 2016. "Excellence in practice through a socio-technical, open systems approach to process analysis and design," *International Journal of Systems & Society*, (3:1), pp.110–118.

Buechner Jeff. 2020. "A Revision of the Buechner–Tavani Model of Digital Trust and a Philosophical Problem It Raises for Social Robotics," *Information* (11), 48, <https://doi:10.3390/info11010048>.

Cecere, G., Rochelandet, F. 2013. "Privacy intrusiveness and web audiences: Empirical evidence," *Telecommunications Policy*, (37:10), pp.1004–1014, <https://doi:10.1016/j.telpol.2013.09.003>.

Connolly, B. 2020. *Digital trust : social media strategies to increase trust and engage customers*. London Bloomsbury Business.

Corritore, C.L., Kracher, B., Wiedenbeck, S. 2003. "On-line trust: concepts, evolving themes, a model," *Int. J. Hum. Comput. Stud.*, (58), pp:737-758.

Ejjami, R. (2024). *The Digital Evolution Strategies for Overcoming Cybersecurity and Adoption Challenges in French SMEs*. *International Journal For Multidisciplinary Research*.

European Parliament. (2023). *Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI*. <https://www.europarl.europa.eu>.

Gefen, D., D. W. Straub. 2004. "Consumer trust in b2c e-commerce and the importance of social presence: Experiments in e-products and e-services," *Omega*, (32:6), pp.407–424.

Global Digital Trust Insights. (2024). <https://pwc.com>.

Hawlitsek, F., Teubner, T., Weinhardt, C. 2016. "Trust in the Sharing Economy. Die Unternehmung," *Swiss Journal of Business Research and Practice*, (70:1), pp. 26-44. <http://dx.doi.org/10.5771/0042-059X-2016-1-26>.

Isaac, H. 2021. Digital technology, confidence and trust.

Jean McNiff. (2017). Action Research All You Need to Know. (pp211-224). Sage.
<https://uk.sagepub.com>

Jim Boehm, Liz Grennan, Alex Singla, Kate Smaje, (2022). Digital trust: Why it matters for businesses. <https://www.mckinsey.com>

Kling, R., Lamb, R., 1999. "IT and organizational change in digital economies: A socio-technical approach," ACM SIGCAS, Computers and Society, (29:3), pp.17–25.

Kökciyan, N., Yolum, P., 2020. "TURP: Managing Trust for Regulating Privacy in Internet of Things," IEEE Internet Computing, (24), pp.9-16.

Launer, M., Svenson, F., Ohler, D., Meyer, J., 2020, "The Development of Digital Trust – Research Directions" in Digital Trust & Intuition at the Workplace Conference Proceeding of the 4th international Service Management Congress, Ostfalia University, November 10-12, 2020, Suderburg.

McKinsey. 2019. The analytics academy: Bridging the gap between human and artificial intelligence.

McKnight, D.H., Chervany, N.L., 2001. "What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology," International Journal of Electronic Commerce, (6), pp.35 - 59.

Marcial, D.E., Arcelo, A.Q., Montemayor, J.O., & Launer, M.A. (2022). Digital Trust in the Academe: people, software, and hardware. Information Technologies and Learning Tools.

Matthew K. O., Lee E. T., 2001. "A Trust Model for Consumer Internet Shopping, International Journal of Electronic Commerce," (6:1), pp.75-91,
<https://DOI:10.1080/10864415.2001.11044227>.

Mattila, J., & Seppälä, T. 2016. Digital Trust, Platforms, and Policy.

Mittendorf, C., Ostermann, U., 2017. "Private vs. Business Customers in the Sharing Economy - The implications of Trust, Perceived Risk, and Social Motives on Airbnb," Hawaii International Conference on System Sciences.

Möhlmann, M. 2016. "Digital Trust and Peer-to-Peer Collaborative Consumption Platforms: A Mediation Analysis," eBusiness & eCommerce eJournal.

Müller, M.P., Garzon, S.R., Rosemann, M., Küpper, A., 2020. "Towards Trust-Aware Collaborative Business Processes: An Approach to Identify Uncertainty," IEEE Internet Computing, (24), pp.17-25.

OECD Secretariat, 2019, Victors of digital transformation OECD digital economy papers 2019 No. 273 www.oecd.org/going-digital.

Rawat, D.B., Alami, H.E., 2023. "Metaverse: Requirements, Architecture, Standards, Status, Challenges, and Perspectives," IEEE Internet of Things Magazine, (6), pp.14-18.

Renner-Micah, Anthony; Effah, John; and Boateng, Richard, " Understanding business process transformation: an institutionalisation perspective" (2023). UK Academy for Information Systems Conference Proceedings 2023. <https://aisel.aisnet.org/ukais2023/10>

Rose, S., Borchert, O., Mitchell, S., Connelly, S., 2019. Zero Trust Architecture.

Sarno, & Maulidar (2024). Cybersecurity Challenges In The Era Of Digital Transformation A Comprehensive Analysis Of Information Systems. Journal Informatic, Education and Management (JIEM).

Rosemann, M. 2019. "Trust-Aware Process Design. International Conference on Business Process Management,"

Ryan, M. 2020. "In AI We Trust: Ethics, Artificial Intelligence, and Reliability," Sci Eng Ethics, (26), pp.2749–2767. <https://doi.org/10.1007/s11948-020-00228-y>.

S. Mishra and S. Gochhait, "Emerging Cybersecurity Attacks in the Era of Digital Transformation," 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2023, pp. 1442-1447, doi: 10.1109/ICICCS56967.2023.10142357.

The World Economic Forum. (2022). Earning Digital Trust: Decision-Making for Trustworthy Technologies. <https://www.weforum.org>.

United Nations. 2018. The Impact of Digital Technologies. <https://www.un.org>

UN Secretary-General High-Level Panel. 2018. The age of digital interdependence. <https://www.un.org>

Wang, Y., Su, Z., Zhang, N., Liu, D., Xing, R., Luan, T.H., Shen, X.S., 2022. "A Survey on Metaverse: Fundamentals, Security, and Privacy," IEEE Communications Surveys & Tutorials, (25), pp.319-352.

Yin, R. K. (2016). Case study research and application: Design and methods (6th ed). (pp.170-175). Sage. <https://us.sagepub.com>

Yuanyuan Guo. 2022. "Digital Trust and the Reconstruction of Trust in the Digital Society: An Integrated Model based on Trust Theory and Expectation Confirmation Theory," Digit. Gov.: Res. Pract. (3-4: 26, pp.19. <https://doi.org/10.1145/3543860>.

Zhghenti, T., Chkareuli, V., 2021. “Enhancing Online Business Sector: Digital Trust Formation Process,” Marketing and Management of Innovations, (2), pp.87-93.
<http://doi.org/10.21272/mmi.2021.2-07>.