ISACA

Digital Trust: A Modern-Day Imperative

Digital Trust

CONTENTS

ABSTRACT

By examining the elements of digital trust and how it underlies every digital transaction, *Digital Trust: A Modern-Day Imperative* explores the importance of digital trust and the practices that enterprises must perform to achieve and uphold digital trust. This white paper defines digital trust and explains the consumer and provider perspectives of digital trust. It establishes why digital trust is more important now than ever, and it explores what digital trust looks like in practice. It concludes with an exploration of how ISACA professionals are uniquely positioned to provide valuable digital trust-related services.

Introduction

An enterprise can improve its relationship with consumers and customers, enhance its reputation and improve brand loyalty by building digital trust, as enterprises are prioritizing digital transformation and more and more interactions happen online. Seventy-three percent of people believe that trust supports customer loyalty, and 57 percent say that trust leads to revenue growth.[1] Digital trust is a significant factor driving consumers' decisions. A digitally trustworthy enterprise is expected to be reliable, act in ways that protect consumers, and use and protect data in a way that aligns with consumer expectations. Therefore, a digitally trustworthy enterprise:

- Understands the consequences of violating consumer trust and what might violate that trust
- Respects consumer data
- Acts in an ethical manner

Digital trust should be a consideration in all areas of an enterprise—people, technology, processes and the organization—and all products and initiatives should be built with digital trust considered from the start. Although digital trust requires significant iterative work, enterprises that can demonstrate their digital trustworthiness can improve their reputation and have an edge over competitors that are less trustworthy.

What Is Digital Trust?

Trust is at the core of every interaction. People often select businesses, relationships and transactions based on their perception of the trustworthiness of the involved parties. Trust is "assured reliance on the character, ability, strength, or truth of someone or something."[2]

When business was primarily conducted face to face, trust in a business was often based on its performance history and reputation, e.g., the perception of a local store or previous interactions with a person. Trust in today's online world is much more complex. Shaking hands with a customer or service provider is nearly obsolete in a digital world where people can purchase products online and even visit a doctor virtually.

Recent technologies shifted trust from the analog world to the digital world. For example, bank accounts can be opened from a mobile device; it is not required to visit a physical location and meet a banker to open an account. The bank may request certain documentation from account holders to ensure they are trustworthy and who they claim to be, while customers no longer need to physically meet the people who work at that bank to trust them.

Digital trust focuses on how trust manifests in a digital context. ISACA defines digital trust as the confidence in the integrity of the relationships, interactions and transactions among suppliers/providers and customers/consumers[3] within an associated digital ecosystem.

Digital trust focuses on how trust manifests in a digital context.

This includes the ability of people, organizations, processes and technology working together to create and maintain a trustworthy digital world. Information is also a critical component of trust, but it underlies people, organizations, processes and technology.

[1] PwC, "The Complexity of Trust: PwC's Trust in US Business Survey," 16 September 2021, https://www.pwc.com/us/en/library/trust-in-business-survey.html
[2] Merriam-Webster, "trust," https://www.merriam-webster.com/dictionary/trust
[3] In this paper, "consumers" refers to customers, users, employees or anyone to whom a supplier or provider gives a good or service; providers refers to any entity that provides a good or service, including suppliers and vendors.

In the context of digital trust, integrity refers to the "adherence to a code of especially moral…values,"[4] and is not the definition of integrity that is used in a security context (i.e., that information is free from unauthorized alteration). The digital trust definition emphasizes relationships, interactions and transactions, which encompass a variety of situations and interaction frequencies, i.e., relationships are typically built around recurring interactions and transactions, each of which may be one-time events.

Digital trust is not interchangeable with confidence. The digital trust definition includes confidence, but digital trust is more all-encompassing than confidence. Confidence is "faith or belief that one will act in a right, proper, or effective way."[5] Digital trust considers relationships, interactions and transactions, but confidence focuses mostly on interactions and transactions. Digital trust also considers an entire ecosystem—people, processes, organizations and technology—but confidence is typically between only a consumer and one enterprise.

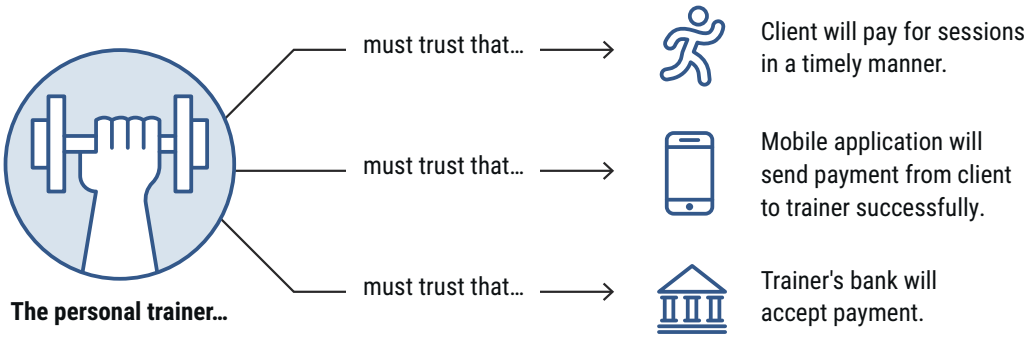
When considering digital trust, it is important to consider the entire digital ecosystem. Interactions often involve more than two parties. Just one untrustworthy party can cause significant harm. **Figure 1** shows how a personal trainer, who accepts payment through a peer-to-peer payment application, needs to trust many parties.

Figure 1 shows that trust encompasses people, organizations, processes and technology, and the underlying information. If any of these elements fail, the integrity of the entire transaction can be questioned, e.g., if the client is trustworthy, but the mobile application malfunctions, trust is diminished for the trainer-client relationship, even though the client was not at fault. One element that is incredibly trustworthy cannot balance out another untrustworthy element, i.e., untrustworthy processes and technology in the hands of very trustworthy people still diminishes digital trust.

Digital trust is not interchangeable with confidence.

Digital trust relates to security, privacy, risk, assurance, quality and governance practices. Each of these tenets contributes to, and can uphold, digital trust. For consumers to find an enterprise digitally trustworthy, they expect that the enterprise has adequate security and privacy controls in place. Effective risk management can help to prevent or limit the number and severity of vulnerabilities. Assurance works to detect issues before they materialize, which can limit potential damage to an enterprise. Without quality efforts in place, consumers may purchase or use faulty products or services, or not receive information that they need, which significantly diminishes trust.

FIGURE 1: Example Digital Trust Ecosystem



[4] Merriam-Webster, "integrity," https://www.merriam-webster.com/dictionary/integrity
[5] Merriam-Webster, "confidence," https://www.merriam-webster.com/dictionary/confidence

Finally, effective governance drives the entire digital trust program, ensuring that digital trust activities achieve their goals and enhance trust with consumers. Those enterprises that have robust security, privacy, IT risk, IT assurance and I&T governance practices are likely to be considered digitally trustworthy. Enterprises need to demonstrate trustworthy characteristics and embed digital-trust consideration throughout their organizations to ensure lasting digital trust.

In addition to these tenets, enterprises need to display particular characteristics to be considered digitally trustworthy, such as integrity, ethics, transparency and accountability. Consumers and customers prefer working with enterprises that act ethically and with integrity. Although ideas about ethics and integrity can vary, enterprises that meet the standards of their consumers and customers are more likely to be considered trustworthy. One commonly observed action taken by digitally trustworthy enterprises is that they clearly communicate their data collection and processing practices, and, when trust-affecting events happen, these enterprises take accountability and clearly communicate any impact to consumers.

Even enterprises that are not technology focused are expected to be digitally trustworthy. Consumers expect some degree of digital trust from every organization with a digital footprint—from a small independent bookstore with an online ordering system, to ubiquitous social media sites. Any enterprise that collects information (e.g., contact details and billing information) or provides a digital service needs to prioritize earning digital trust.

Any enterprise that collects information (e.g., contact details and billing information) or provides a digital service needs to prioritize earning digital trust.

Obtaining digital trust is not a one-time activity; the definition of digital trust focuses not only on the creation but also on the maintenance of a trustworthy digital ecosystem. Trustworthy enterprises work continuously to build and maintain trust by regularly evaluating the current state of digital-trust practices and taking action to address any areas of weakness.

Why Does Digital Trust Matter?

It is estimated that 2.5 quintillion bytes of data are produced daily.[6] This data can reveal a lot about individuals' lives and habits. An insignificant Facebook® like can reveal enough information to predict an individual's political views.[7] With the spike in personal information that is being shared online through practices such as telehealth, significant harm can result from information not being protected properly.

Data are not just random 1s and 0s; they represent the most personal details of a person, e.g., location, lifestyle, health and family information. Although anonymization may give consumers a sense of security, it is still possible to identify a person from data sets that are stripped of information.[8] Therefore, it is almost impossible for people to not have comprehensive and accurate digital profiles, which highlights the importance of digital trust.

Data are not just random 1s and 0s; they represent the most personal details of a person.

Given the highly sensitive information that data can reveal and the consequences if this information is revealed, trust is foundational for an individual to be comfortable leveraging a service that requires sharing personal information. Seventy percent of people polled say trusting a brand is more important now than it was in the past—trust is the second biggest factor when purchasing from a

[6] Seed Scientific, "How Much Data Is Created Every Day? [27 Staggering Stats]," 28 October 2021, https://seedscientific.com/how-much-data-is-created-every-day/#:~:text=How%20much%20content%20is%20created,2.5%20quintillion%20bytes%20of%20data

[7] Praet, S.; P. Van Aelst; P. van Erkel; S. Van der Veeken; D. Martens; "Predictive modeling to study lifestyle politics with Facebook likes," EPJ Data Science, 2 October 2021, https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-021-00305-7

[8] Kolata, G.; "Your Data Were 'Anonymized'? These Scientists Can Still Identify You," The New York Times, 23 July 2019, https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html

new brand.[9] Digital trust extends beyond information being improperly collected or disclosed. Insecure sites and downtime can also tarnish trust. Outages can prevent customers from receiving goods, services or information they need. For example, if an online pharmacy is hacked and is experiencing extended downtime, people may be unable to order important medication they need. The insecure website downtime can affect customers' health, which makes them lose trust.

Digital Trust: Consumer Perspective

Many consumers' and customers' decisions are based on trust. Consumers consider six factors when determining digital trust:

- Quality
- Availability
- Security and privacy
- Ethics and integrity
- Transparency and honesty
- Resiliency

Quality

Consumers expect that a product, service or asset they receive is of expected quality. The expected quality may not be high quality. Consumers may select a product that they know is inferior, based on cost or another consideration, but the consumer expects to receive something that is at or exceeds the expected level of quality. If the quality of the product, service or asset that is received does not meet consumer expectations, trust may be damaged, and the consumer may choose not to do further business with the provider.

Availability

Consumers may depend on information from a provider, and that information should be available and accurate. Not being able to access information can negatively affect consumers.

For example, if a bank application is broken and does not show account balances, a consumer may be unaware that a small purchase will overdraw their bank account.

Inaccurate information is as harmful as unavailable information and affects trust. Inaccurate information can lead consumers to make decisions that can cause damage. For example, if a navigation application is not updated with new road information or road conditions, drivers can get lost or drive on unsafe roads.

Security and Privacy

Consumers often supply information, e.g., email addresses and billing information, to providers and expect that this information is kept secure and private. A provider should clearly communicate to consumers how their provided information is used. For example, a provider should communicate to consumers that the email addresses that they provide for shipping updates may also be shared with marketing teams.

Information and systems need to be adequately secured. If sufficient controls are not in place to protect information throughout its life cycle, consumers can suffer harmful consequences, such as identity theft or privacy violations. Consumers need providers to destroy information when it is no longer needed and, if it is needed, securely retain it for an appropriate amount of time.

If sufficient controls are not in place to protect information throughout its life cycle, consumers can suffer harmful consequences, such as identity theft or privacy violations.

For example, if a banking application is not secured, a user's funds can be drained, creating significant hardship for that person and diminishing his or her trust in the bank.

[9] Edelman, "Trust Barometer Special Report: Brand Trust in 2020," 25 June 2020, https://www.edelman.com/research/brand-trust-2020

Ethics and Integrity

Another factor that consumers consider for digital trust is whether providers act ethically and with integrity. Although some expectations and thresholds may vary, depending on the context and from consumer to consumer, enterprises should act in a way that supports the ethics and values of their customers. Consumers may select a provider because it aligns with their values, but if the provider pivots from those values, that trust can erode. For example, if a messaging application is introduced to the market with security and privacy core values, but then it shares excessive information with third parties, digital trust is harmed because users joined the application for its security and privacy benefits.

Transparency and Honesty

Transparency, honesty and accountability are also consumer considerations for digital trust. Consumers want to know what is happening with their data and how their data are being used. Communicating clearly with consumers about their data is a key practice to demonstrate transparency. If consumers are not technical, enterprises should provide notices in nontechnical language that is easily understandable. Transparency, honesty and accountability are especially important in the event of a breach or incident: Admitting the breach and clearly and proactively communicating with consumers about the breach can help to insulate the reputational harm that breaches cause.

Stability and Resilience

Organizations must be resilient to negative external influences to be trustworthy. Consumers need to believe in the stability and resilience of an enterprise to develop a relationship with it. To be stable and resilient, an enterprise should be able to keep up with a changing business and technology landscape. Refusal to evolve or try new technologies may result in an enterprise that is not using state-of-the-art security and privacy technologies, and they may not be able to keep information secure and private, which tarnishes trust.

To be stable and resilient, an enterprise should be able to keep up with a changing business and technology landscape.

And though consumers expect providers to change with the times, they also expect some degree of stability. For example, if a provider typically has excellent customer service but errors resulting from a redesign of their mobile application causes a significant breakdown and degradation of their customer service, digital trust will likely be affected.

Digital Trust: Provider Perspective

Enterprises should value digital trust because it can provide a competitive advantage over enterprises that are not considered trustworthy. It is imperative for enterprises that seek to build relationships with consumers prioritize trust. Trust is also critical to every enterprise's bottom line. Consumers who have trusted a brand for a long time are more likely to buy from that brand first, stay loyal to it, advocate for it and defend it, compared to consumers who do not fully trust a brand.[10]

Part of being a digitally trustworthy enterprise includes providing accurate and consistent, i.e., valid, information to a product or service provider. As discussed previously, inaccurate information can lead to significant harm for consumers, but providing inaccurate information for product input or to service providers can be equally damaging. For example, if a vendor provides inaccurate bank routing information to an enterprise, the vendor may not get paid, which can lead to a damaged relationship

[10] Edelman, "In Brands We Trust?" 2019, https://www.edelman.com/sites/g/files/aatuss191/files/2019-06/2019_edelman_trust_barometer_special_report_in_brands_we_trust.pdf

between the vendor and the enterprise, and affect future dealings. Providing accurate and consistent data to products or service providers may include soliciting consumer feedback, conducting regular assessments and updating information as appropriate.

Although most providers work with third parties in some capacity, trusted providers must carefully determine the third parties with whom they share information. Providers should only share the information that is needed to carry out a transaction with goods/service providers. It is also imperative that providers work with trustworthy third parties. Digital trust must be present across the entire supply chain. If a consumer's information is breached as a result of a neglectful third party, the consumer is likely to be upset with the provider and the third party. In such cases, consumers are often unaware that a third party was the weak link, and all reputational harm falls on the provider. For example, the breach affecting retailer Target is often referred to as the Target breach, even though the breach resulted from one of Target's compromised vendors.

Digital trust must be present across the entire supply chain. If a consumer's information is breached as a result of a neglectful third party, the consumer is likely to be upset with the provider and the third party. In such cases, consumers are often unaware that a third party was the weak link, and all reputational harm falls on the provider.

Third-party systems and processes must also be secure. If a third party does not have proper change management processes in place, it may inadvertently use old code that has vulnerabilities. It is also critical that third parties have adequate patch management practices in place. A majority of breach victims indicate that they were breached because of an unpatched known vulnerability.[11]

Digital Trust in Practice

One of the most important elements of digital trust is transparency, specifically transparency about how data collected from consumers are used and transparency in the event of a breach. Freely given consent from consumers to collect their data is foundational to transparency. Using dark patterns, which are techniques to trick or influence data subjects to make a specific choice[12] is antithetical to trust.

Freely given consent from consumers to collect their data is foundational to transparency.

Many dark patterns are manifested in user-experience design, e.g., displaying a grayed-out "Opt out of tracking" button on the user interface that it looks like it is not available to be clicked. Tricking users into giving consent to use their data, i.e., an obscuring data-handling practice, violates digital trust and must be avoided.

The type of information that an enterprise collects may affect the controls that the enterprise applies to best protect that information, so it is critical that organizations have an understanding of the data that they collect and the data sensitivity. Regular audits can help enterprises ensure that controls are in place and operating as intended. Controls can prevent mishaps that tarnish digital trust by anticipating failures before they materialize. An enterprise that takes steps to address vulnerabilities before they lead to harm can build its reputation as a trustworthy organization.

Security is foundational to digital trust; if the information that a consumer shares with a provider cannot be protected, trust cannot be ensured. Enterprises must ensure that they know what data they collect and apply appropriate safeguards based on the type of data. Boards of directors must value security, and security must be prioritized and governed properly.

[11] Service Now, "Costs and Consequences of Gaps in Vulnerability Response," https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html
[12] Morrison, S.; "Dark patterns, the tricks websites use to make you say yes, explained," Vox, 1 April 2021, https://www.vox.com/recode/22351108/dark-patterns-ui-web-design-privacy

Although consumers expect strong security for the information they provide, breaches may happen. Providers must document incident response plans that include communication considerations.

When a breach occurs, transparency, accountability and communication are critical to limit damage to the reputation of the enterprise and digital trust. Intentionally minimizing the scale of a breach or attempting to hide its occurrence can cause reputational damage and tarnish trust.[13] Customers would rather hear about breaches from the affected enterprises than from the news,[14] therefore, honest communication about breaches is imperative.

Enterprises should also consider that their employees may be considered consumers or customers in certain cases, and digital trust between employee and employer is critical. For example, providing untrustworthy technology to employees that makes it difficult to do their jobs or monitoring employees without their knowledge and consent could harm digital trust between employees and employers, leading to disgruntled employees, who can be a significant threat to enterprises.[15]

Where Does ISACA Fit In?

ISACA professionals are global IT audit, governance, security, risk and privacy experts. All ISACA-affiliated professionals are digital-trust practitioners, because each ISACA core domain facilitates digital trust. Digital trust cannot exist or be assured without audit, governance, security, risk and privacy; therefore, professionals in these fields are ultimately working toward supporting digital trust. All of these domains are key partners in supporting digital trust; no one domain alone can work in a silo to ensure digital trust exists.

An enterprise may have excellent digital-trust plans in place, but if it does not audit, monitor and assess the technology and systems that support those plans, digital trust objectives will most likely not be met. Regularly monitoring and auditing digital-trust-related technology and practices can help prevent breaches of trust, which can help prevent reputational damage.

An enterprise may have excellent digital-trust plans in place, but if it does not audit, monitor and assess the technology and systems that support those plans, digital trust objectives will most likely not be met.

IT governance "consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives."[16] Effective governance is key to the success of a digital-trust initiative because effective governance ensures that digital trust is considered holistically, and accounted for and supported throughout the enterprise. Digital trust should align with other enterprise goals. A strong governance program can help to ensure that enterprise priorities support digital trust (and vice versa).

Security is built on the confidentiality, integrity and availability (CIA) triad (see **figure 2**). In exchange for providing their information, consumers expect that their information is kept confidential and only shared if absolutely necessary. Consumers also expect that their information is kept accurate, because inaccuracies can cause harm and damage trust. It is critical that information is available to consumers when they need it. Frequent system outages or other unavailability can tarnish digital trust and cause consumers to choose a more reliable provider.

[13] Davis, J.; "How not to handle a data breach brought to you by Uber, Equifax and many others," Healthcare IT News, 1 October 2018, https://www.healthcareitnews.com/news/how-not-handle-data-breach-brought-you-uber-equifax-and-many-others
[14] Bertucci, D.; "Data Breach Notifications and Why Honesty is the Best Policy," InfoSecurity Magazine, 24 April 2018, https://www.infosecurity-magazine.com/blogs/data-breach-notifications-honesty/
[15] Mitchell, J.; "Disgruntled employees pose greatest cyber-security risk, warns expert," MyBusiness, 1 November 2021, https://www.mybusiness.com.au/technology/8482-disgruntled-employees-pose-greatest-cyber-security-risk-warns-expert
[16] ISACA Glossary, "IT Governance"

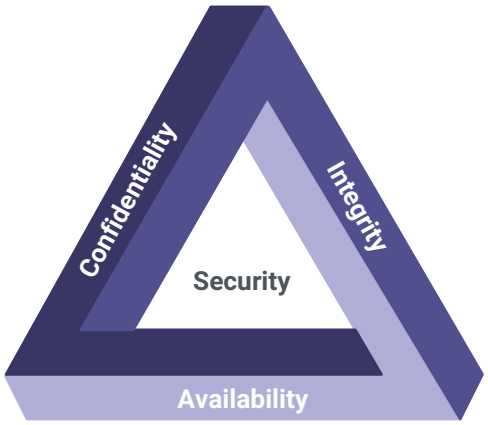
Preserving digital trust requires enterprises to anticipate and address any risk that can affect digital trust. When enterprises are determining if they should avoid, transfer, mitigate or accept risk, digital trust should be a factor in risk response. Senior leaders should consider how risk decisions affect digital risk. For example, if a particular risk is accepted, an enterprise should answer the following questions:

- How does accepting that risk affect digital trust?
- Will the acceptance of that particular risk result in harm or loss to an asset or group of assets that, if realized, have an adverse impact on consumers?

An enterprise that has earned digital trust is expected to keep information private and only collect the minimum amount of information necessary. **Figure 3** shows the privacy engineering objectives of predictability, manageability and disassociability, which directly relate to digital trust.

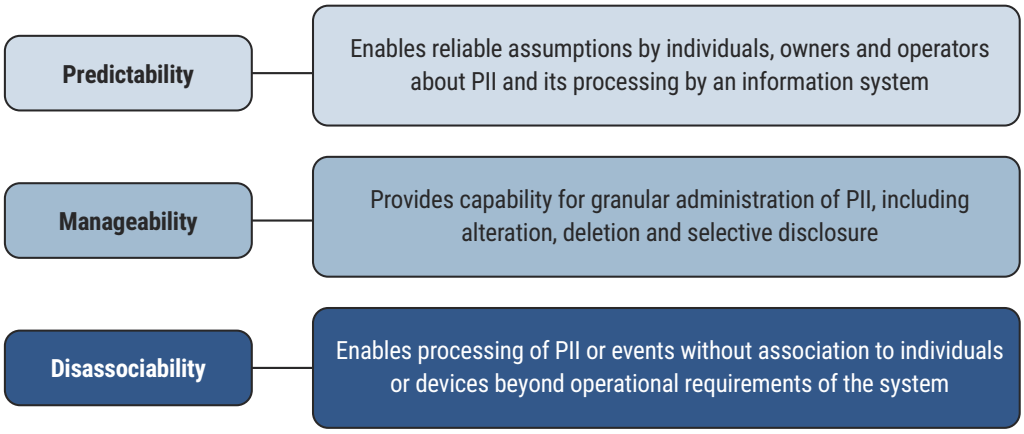
Predictability, which relates to transparency, ensures that the way in which information is processed is predictable and that assumptions about data handling are accurate. Predictability is critical to digital trust, because if consumers have an expectation of how their data are processed and how their data are used, deviations will damage trust. Manageability is the ability to modify and selectively disclose information. Inaccurate information can undermine trust, e.g., a healthcare provider has incorrect contact information for a consumer and discloses medical information to the wrong person. The ability to rectify inaccuracies must be possible if digital trust is to be upheld. Because data can reveal significant sensitive information about people, the ability to process this information without attributing it to individuals, i.e., disassociability, is key—enterprises that can successfully disassociate data can gain the trust of their customers.

FIGURE 2: Security Engineering Objectives



Source: ISACA, *Cybersecurity Fundamentals Study Guide, 3rd Edition*, USA, 2021, figure 1.11, https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KohiEAC

FIGURE 3: Privacy Engineering Objectives



Source: NIST, "An Introduction to Privacy Engineering and Risk Management in Federal Systems," NISTIR 8062, January 2017, https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

Conclusion

Due to the growing amount of data that are generated by people daily, it is imperative to protect those data and use them ethically. Consumers understand the harm that improper handling of their information can cause, so digital trust is not optional. Enterprises that want to survive must value digital trust.

Reputation is critical to enterprises. Although earning a good reputation is challenging, enterprise reputation can be damaged quickly with one harmful incident.[17]

Digital trust is an iterative process. Enterprises must constantly evaluate their digital trust practices and adjust them when areas for improvement are identified.

Enterprises that can demonstrate their digital trustworthiness gain considerable competitive advantage and build better relationships with consumers.

[17] Blanchard, P.; "The Importance of Brand Reputation: 20 Years to Build, Five Minutes to Ruin," Forbes, 27 December 2019, https://www.forbes.com/sites/forbesagencycouncil/2019/12/27/the-importance-of-brand-reputation-20-years-to-build-five-minutes-to-ruin/?sh=6cfd5f022e69

Acknowledgments

ISACA would like to acknowledge:

Expert Reviewers

Jo Stewart-Rattray
CISA, CISM, CGEIT, CRISC, FAISA, FACS CP(Cyber)
Australia

Sanja Kekic
CRISC, CDPSE
Serbia

Board of Directors

Gregory Touhill, Chair
CISM, CISSP
Director, CERT Division of Carnegie Mellon University's Software Engineering Institute, USA

Pamela Nigro, Vice-Chair
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision, USA

John De Santis
Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Niel Harper
CISA, CRISC, CDPSE, CISSP
Former Chief Information Security Officer and Privacy Officer, United Nations Office for Project Services (UNOPS), Denmark

Gabriela Hernandez-Cardoso
Independent Board Member, Mexico

Maureen O'Connell
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Veronica Rose
CISA, CDPSE
Founder, Encrypt Africa, Kenya

David Samuelson
Chief Executive Officer, ISACA, USA

Gerrard Schmid
President and Chief Executive Officer, Diebold Nixdorf, USA

Asaf Weisberg
CISA, CISM, CGEIT, CRISC
Chief Executive Officer, introSight Ltd., Israel

Tracey Dedrick
ISACA Board Chair, 2020-2021
Former Chief Risk Officer, Hudson City Bancorp, USA

Brennan P. Baybeck
CISA, CISM, CRISC, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Rob Clyde
CISM
ISACA Board Chair, 2018-2019
Independent Director, Titus, and Executive Chair, White Cloud Security, USA

About ISACA

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams that effectively drive IT audit, risk management and security priorities forward. ISACA is a global professional association and learning organization that leverages the expertise of more than 150,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide. In 2020, ISACA launched One In Tech, a philanthropic foundation that supports IT education and career pathways for under-resourced, under-represented populations.

DISCLAIMER

ISACA has designed and created *Digital Trust: A Modern-Day Imperative* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Provide Feedback:

www.isaca.org/digital-trust-modern-day-imperative

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/