IN PURSUIT OF DIGITAL TRUST

Why Digital Trust is Crucial to You and Your Enterprise

Karen Heslop, JD, CDPSE, VP Content Development, ISACA
After completing this session, you will be able to:

- Define digital trust
- Detail the digital trust ecosystem
- Explain both the consumer/user and provider perspectives in the digital trust ecosystem
- Describe how ISACA fits into the digital trust ecosystem and why it is a key partner in this area
Sample Scenarios
Digital Trust is needed in all relationships that evolve in a digital ecosystem. The trust required extends beyond the trust in the technology to include the people, process, and organization.

### Digital Trust Use Cases

<table>
<thead>
<tr>
<th>Relationship</th>
<th>Service Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business to Consumer (B2C)</td>
<td>A consumer engages with an app for e-banking</td>
</tr>
<tr>
<td>Business to Business (B2B)</td>
<td>Outsourcing cloud services</td>
</tr>
<tr>
<td>Business to Employee (B2E)</td>
<td>The handling of payroll data</td>
</tr>
<tr>
<td>Business to Government (B2G)</td>
<td>Submitting enterprise tax statements</td>
</tr>
<tr>
<td>Government to Constituent (G2C)</td>
<td>Vote collection and tallying</td>
</tr>
</tbody>
</table>
What is Digital Trust?
It Starts With Trust

Trust is assured reliance on the character, ability, strength, or truth of someone or something.

Digital trust focuses on how trust manifests in a digital context.
Digital Trust is Prevalent in Current Headlines

NEWS ANALYSIS

What is digital trust? How CSOs can help drive business

What is digital trust and why does your CSO care about it?

A 5-step approach to building digital trust through cybersecurity

Digital trust: business buzzword or the future for cybersecurity?
Sample DT Definitions

**World Economic Forum:** Digital Trust is a necessity in a global economy reliant on ever-increasing connectivity, data use, and new innovative technologies. In order to be trustworthy, technology must be secure (ensuring connected systems’ confidentiality, integrity, and availability) as well as responsibly used.

**Accenture:** Accenture defines digital trust as the confidence placed in an organization to collect, store, and use the digital information of others in a manner that benefits and protects those to whom the information pertains.

**Security Magazine:** In simple terms, digital trust can be defined as the confidence people have in an organization’s ability to keep their digital data secure and to handle it with integrity and accountability.

Many frame digital trust in terms of security, but ISACA thinks it is greater than that.
ISACA Definition

Digital trust is the confidence in the integrity of the relationships, interactions and transactions among providers and consumers within an associated digital ecosystem. This includes the ability of people, organizations, processes, information and technology to create and maintain a trustworthy digital world.

- Breaking down the definition
  - Not interchangeable with confidence
  - Integrity refers to a code of moral value (not traditional security definition)
  - Must consider the entire ecosystem; interactions often involve more than two parties
  - Security, privacy, risk, assurance, quality and governance contributes to, and can uphold digital trust
  - Ethics, transparency and accountability also play a role
  - Encompasses brand, product quality, data ethics and reliability
Business Benefits

Digital Evolution

- Next progression in digital transformation
- Driven by business needs to enable companies to remain competitive and meet customers’ expectations

Why should enterprises focus on digital trust?

- Digital trust is a significant factor driving consumers’ decisions
- It helps to improve enterprises’ reputation
- Drives customer loyalty
Digital Trust Ecosystem
Why an Ecosystem?

- Enterprises don’t operate in a vacuum
- Dependence on third-party goods and services
- Key stakeholders in the ecosystem:
  - Service/Product/Information provider
  - Service/Product/Information consumer
  - Third-party Service/Product/Information providers
  - Proxy technology
  - Digital peers
Ecosystem Participant Expectations

**Consumer**
- The products, services or assets they receive from the provider are as expected.
- The information on which users depend is available, accurate, complete, consistent and timely, and information integrity is assured (not just from a security angle).
- The information that is supplied to the organization is secure and securely disposed when no longer needed, and privacy is ensured throughout the life cycle. Also, all internal data should be protected.
- The organization(s) involved in the relationship operates with high ethics and integrity (human rights; ethical use of technology; diversity, equity and inclusion (DEI); etc.) and offers its products or services in a sustainable manner.
- The organization is transparent, honest and accountable.
- The organization is resilient to negative external influences.

**Provider**

**Consumer relationship**
- Providing accurate and consistent (valid) information to the product/service provider
- Divulging this information to obtain the intended goods or services
- Assuming that the enterprise for whom they are divulging information will honor and maintain a fiduciary duty with respect to that information

**Third-party relationship**
- Provides only necessary, minimized information to the provider to process a transaction or provide the transactional service
- Appropriately manages data to ensure that it is secured and disposed of when no longer needed
ISACA’s Role in Digital Trust
All ISACA-affiliated professionals are digital-trust practitioners
Digital Trust Ecosystem Framework

New Digital Trust Ecosystem Framework (DTEF) harnesses pillars of digital trust

- Digital trust central to ISACA’s mission; DT is the next area of focus for enterprises on their digital transformation journey
- A 3D model that recognizes interconnectivity of the components parts and contemplates that a change in one part impacts other part(s)
- Systems thinking underlies DTEF
- Complements existing frameworks and standards
- Exposure draft in April
- Expected to be finalized by Q4 2022
Digital Trust Ecosystem Framework: Sneak Peek
Nodes

Four Nodes:

- People
- Process
- Technology
- Organization
Six Domains:

- Culture
- Emergence
- Human Factors
- Enabling & Support
- Direct & Monitor
- Architecture
DTEF Structure

Children of Domains include:

- Trust Factors
- Practices
- Activities
- Outcomes
Final Thoughts

Digital Trust is an obvious and easy concept, but its practical application is far more difficult to implement and quantify.

Its relevance is widespread and has huge implications for enterprises, individuals (consumers, customers, users) and all involved in the larger digital ecosystem.

ISACA is trying to fill the void with its new framework on this important topic.
Thank you!