How Digital Trust Drives Culture Change

Privacy is a right, not a privilege. But organizations and leadership often struggle when it comes to adapting their culture toward digital trust and stewardship.
How Digital Trust Drives Culture Change
CHON ABRAHAM, RONALD R. SIMS, SALLY DAULTREY, ANNE BUFF, AND ANNE FEALEY

Privacy is a right, not a privilege. But organizations and leadership often struggle when it comes to adapting their culture toward digital trust and stewardship.

We have entered a critical moment in the evolution of the digital economy where we must question where and how personal data should be used and determine who has the right to gain commercial profits from the insights generated by users’ digital data. Organizations must think critically about their own digital trust — an umbrella term we use to describe the behavioral guidelines and cultural principles that include data privacy, security, protection, and stewardship.

Beliefs and behaviors in today’s virtual world blur the definitions and boundaries of responsibility for data privacy, which is reshaping consumers’ expectations of protection. Organizations seeking to adapt their culture toward better digital trust face many challenges. By identifying a topology of behaviors and attitudes of different kinds of companies, we have determined four techniques that organizations can use to map their journey from compliance to trust.

Investigating Digital Trust
When an organization goes through a privacy and breach disclosure effort, actions are typically driven by compliance requirements and regulatory changes, while the underlying culture around digital trust within the organization often remains unchanged. For every

The past year has been critical for Facebook’s reputation, with the tech giant coming under scrutiny following extensive, high-profile data privacy breaches. The failure of Facebook to provide good answers to tough questions about how and why it uses citizens’ data has exposed the cracks in the trust infrastructure that underpins our digital economy. Today, companies can be considered “cybersecure” but still not employ processes that ensure the security of internal data and the integrity of data relations with external stakeholders.
interaction where data is shared between a private individual and an organization, there is an implicit zone of trust created between the parties. The fallout from recent data breaches — whether due to apparent disregard for citizens’ data or inadvertent disclosure — suggests appraisal of this trust relationship is overdue. The introduction of formal measures may enable organizations to differentiate themselves on a scale for digital trust (similar to the Ponemon Institute trust rankings, promoting and perhaps incentivizing digital trust across the business ecosystem.

In December 2017, we surveyed 83 members of a U.S. consortium of information technology and security executives to understand what goes on in their companies in the context of digital trust and to explore their attitudes toward data privacy and breach disclosure. We also interviewed 60 senior executives from public and private sector organizations who already had data breaches and were actively engaging in prevention activities. Both groups are highly representative of organizations that recognize their culture must adapt toward better digital trust.

Out of 83 responses, just more than half (54%) were confident that their organization goes beyond the basics to achieve best practices. Only 39% were satisfied that their organization is at least compliant. Fifty-four percent reported they were satisfied with their organization’s current culture of breach notification but recognized that more can and should be done to protect the organization’s brand if a lapse in breach disclosure responsibility inadvertently occurs. Sixty-three percent believed their industry generally to be compliant, largely due to fear of being publicly exposed in the media. A few believed that public scrutiny in breach reporting encourages compliance but noted that compliance is not the same as cybersecurity or ethical data privacy safeguards.

Attitudes toward digital security and trust among those we surveyed also depended on industry contexts. In the health care industry, for example, respondents noted that because their organization had never been publicly shamed, they surmised that their data security and data privacy practices were “good enough.” Particularly for health care organizations, this indicates a risk of being closed to proactive cybersecurity strategy, suggesting that more-passive organizations may be one hack away from a damaging breach, data spillage, or unsanctioned data use.

We identify four organizational cultures along a continuum of digital trust: from conditions of ignorance and neglect, to defiance, to compliance, to integrity (see “The Digital Trust Culture Continuum”). These cultures can account for an organization’s downfall — or save it from self-destruction. Companies that move away from a culture of ignorance and neglect toward one of integrity should start by investigating the underlying group behaviors and information exchange habits in the organization. Often, these behaviors and habits indicate the root cause for failures in digital trust. A major challenge for companies is the slow rate of change in organizational culture and the difficulty involved in accomplishing measurable progress, in large part because change is more often and more easily spurred by external, not internal incentives.
The Digital Trust Culture Continuum

**Ignorance and Neglect**
- Fails to observe basic criteria for creating digital trust (for example, notification about data usage under data privacy laws and breach notification standards)
- Has weak/no attention to standards or strategy, neglects governance for critical aspects of digital trust (for example, data privacy assurance, mitigation, and breach)

**Defiance**
- Deliberately resists critical aspects for creating digital trust (for example, refusing to abide by data privacy and breach behavior notification laws)
- Acts only because law requires it, conforms to minimum requirements
- Openly acknowledges data usage and selling practices and openly rewards employees’ ethical behavior
- Takes preventive action to safeguard private data even if there is a fiscal impact on business operations (for example, two-factor authentication)
- Exhibits best practice, recognized as benchmarked organization for digital trust

**Compliance**
- May not agree with legal or regulatory aspects critical to digital trust but acts to meet the laws or standards
- Delays and denies guilt in corporate wrongdoings associated with private data usage
- Exhibits best practice, recognized as benchmarked organization for digital trust

**Integrity**
- Deliberately includes digital trust in corporate strategy
- Is committed to exceeding the minimum compliance required by law, exhibits ethical conduct such as consumer education on credit protection, awards financial compensation to consumers affected by, for example, unauthorized private data usage
- Takes preventive action to safeguard private data even if there is a fiscal impact on business operations (for example, two-factor authentication)
- Exhibits best practice, recognized as benchmarked organization for digital trust

**Source:** Adapted from W.I. Sauser, Jr., “Crafting a Culture of Character: The Role of the Executive Suite,” 2008.
Driving Culture Change With Incentives

Other than California’s Consumer Privacy Act (CCPA) of 2018 specifically for data privacy, state laws typically cover only exfiltration of data that is likely to cause hardship for the consumer. These data breach laws are inherently reactive and do not address misuse or undisclosed use of consumer data. The stipulations of the laws differ across state lines in terms of criteria for companies and varying definitions of “consumer.”

Incentivizing digital trust in ways that move entire social and business ecosystems toward a culture of integrity will require government fiscal measures and methods for data monetization. Historically, the tool of choice for government has been penalties and fines; however, to drive cultural change, incentives are more likely to be effective than penalties. Penalties punish an action after the fact rather than reward good behavior. For example, via the HITECH Act of 2009, the government fined health organizations for not meeting baseline metrics in digitizing medical data, which spurred organizational cultures of compliance. While national incentive payments are highly unlikely for digital trust, tax breaks make sense for most businesses. To establish such tax breaks, metrics based on a societal norm for privacy must be established to gauge digital trust.

Many of the 23 national and federal U.S. policies on cybersecurity already contain elements that could be useful in framing metrics on digital trust, such as the 2014 U.S. Cybersecurity Enhancement Act. Implementation costs for cybersecurity and the need for simplified frameworks deter companies from achieving and exceeding compliance. Implementation is difficult without incentive or regulation. In this era of government deregulation, or at best slow reactive regulation (for example, consider the congressional and state reactions, with the exception of California, to Facebook’s Cambridge Analytica scandal), much is left to the individual organization and business ecosystem to drive cultural change in digital trust.

The nefarious market for the sale of consumer private data among companies without the knowledge of consumers is dubious enough. Other acts are questionable, such as the upselling of security features to consumers that should probably be free or discounts to consumers if they opt in for use of their data. No one should have to pay for baseline privacy — a corporate responsibility for digitally transacting with consumers. Privacy is a right, not a privilege.

However, companies consider monetizing consumer data privacy services as within their business rights. Given this, why not incentivize consumers to be more proactive in demanding organizations to invest in digital trust? We recognize this is a significant paradigm shift that will require innovative thinking and challenge traditional business models. Changing consumer privacy behaviors with incentives is likely to be far more effective and quicker than changing organizational behaviors. One possibility is to start with social media consumers to whom government can offer a personal tax reduction or percentage decrease on federal student loans, however small, for proof of opt-out contractual options for personal (nonprivate) data sharing. The government could create a self-selected protected group (akin to the Federal Trade Commission’s do-not-call and do-not-email registries). Those who opt out of sharing personal (nonprivate) data and information are
incentivized. This serves as not only a positive for consumer data protection but also a benefit for businesses by shifting the responsibility (or at least a portion) of data protection to the consumer. Small steps can spur greater behavior changes.

**A New Awareness of Organizational Culture**

Whether stakeholders are internal or external to the organization, maintaining their trust is a critical component of a responsible organizational culture. Therefore, responsibility for digital trust falls partially on organizations; they must be proactive in investigating their internal behaviors and knowledge ecosystems, measuring not only how and where data is exchanged but how those vectors are valued within the organization. Leaders (principally, the C-suite) should map mechanisms for digital trust to meet both expectations of the people entrusting them with their data and their internal organizational moral compass (for example, the ethical standards for organizational behavior as a manifestation of its core values and policies). It is every company stakeholder’s responsibility to follow the moral compass institutionalized in its culture.

We suggest that organizations can benefit from four activities in their journey toward better digital trust:

1. **Recognize that cybersecurity and privacy are only part of the story.** To safeguard individuals and the collective organization, cybersecurity compliance frameworks and data privacy/cybersecurity hygienic behaviors provide a useful foundation for identifying pathways to better digital trust. Such frameworks and behaviors should continue to be refreshed and revised because the digital space changes constantly. Organizations can map and identify where data lives in the organization to understand what core functions, transactions, processes, and business advantages depend on the data and to establish processes to review new uses of the data, new places where the data is stored, and new data created or collected by the organization.

2. **Analyze where and how behavior change has occurred in the organization.** In changing a culture, no organization starts from zero. Leaders can look to the past, identify change agents and knowledge elites that serve the interests of digital trust, seek where groups cross organizational boundaries and structures, and work with these, not against them.

3. **Know the scope and reach.** It is important to measure the scope and reach of the digital contract of trust. This is critical and depends on data identifying where context and value challenge expectations and outcomes.

4. **Define the terms of the company’s social license to operate in the digital economy.** The license should be clearly stated and easily accessed on the company’s website and in all digital correspondence with its customers and business partners. Leaders should explain how the company earns and maintains trust of private individuals and business partners and establish regular reviews (biannually at minimum) to update terms to address shifts in consumer expectations.

Organizations that wish to retain their social license must align their business ambitions with evidence that digital trust is a part of their operations. Definitions of corporate social responsibility (CSR) must expand beyond protecting social and environmental well-being to include protecting digital well-being for consumers and
employees. The vocabulary and principles of the digital trust agreement should be added to requirements for effective leadership in every organization and company in the digital age.
About the Authors

Chon Abraham is an associate professor of information systems at the College of William & Mary's Raymond A. Mason School of Business and a military reserve cyber officer in the U.S. Air Force Chief Data Office at the Pentagon, and researches topics related to national cybersecurity interests. Ronald R. Sims is the Floyd Dewey Gottwald Senior Professor at the College of William & Mary's Raymond A. Mason School of Business. Sally Daultrey is a U.K.-based research analyst specializing in the geopolitics of cyberspace and the role for science in regional security strategy. Anne Buff (@anne_buff) is a strategic adviser and thought leader at SAS. Anne Fealey is a global chief privacy officer and self-described privacy evangelist.

References

1. Social relationships and rights to data privacy were first tested in the 19th century, when the camera became widely available. Photographers could use the likenesses of others without permission, often making money through the sale of images to newspapers and advertisements. See S. Warren and L. Brandeis, “The Right to Privacy,” Harvard Law Review 4, no. 5 (Dec. 15, 1890): 193-220.


5. CCPA, effective Aug. 31, 2018, applies to companies that collect consumers’ personal information (PI), do business in California, and have annual gross revenues in excess of $50 million; annually sell PI relating to 100,000 or more consumers or devices; or derive 50% or more of their annual revenues from selling consumers’ PI. “Consumer” is defined as a natural person who is a California resident (an individual who is in California for other than a temporary or transitory purpose or is domiciled in California who is outside California for a temporary or transitory purpose). More amendments are likely through Jan. 1, 2020. See P.G. Patel, N.D. Taylor, and A.E. Laks, “Less Is Less: California Legislature Amends Limited Aspects of California Consumer Privacy Act,” client alert, Morrison & Foerster, Sept. 4, 2018, www.mofo.com.


7. Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Public Law 111-5, Title VIII.

8. “The DoD Cybersecurity Policy Chart,” Cyber Security and Information Systems Information Analysis Center, updated June 12, 2018. The April 2018 update to the NIST Core Functions that “are not intended to form a serial path, or lead to a static desired end state [but should instead] be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk”; see M.P. Barrett, “Framework for Improving Critical Infrastructure Cybersecurity,” National

9. SANS Institute Editorial Board and archived commentaries.


Articles published in MIT Sloan Management Review are copyrighted by the Massachusetts Institute of Technology unless otherwise specified at the end of an article.

MIT Sloan Management Review articles, permissions, and back issues can be purchased on our website: sloanreview.mit.edu or you may order through our Business Service Center (9 a.m.-5 p.m. ET) at the phone numbers listed below. Paper reprints are available in quantities of 250 or more.

Reproducing or transmitting one or more MIT Sloan Management Review articles by electronic or mechanical means (including photocopying or archiving in any information storage or retrieval system) requires written permission.

To request permission, use our website: sloanreview.mit.edu or Email: smr-help@mit.edu
Call (US and International):617-253-7170 Fax: 617-258-9739

Posting of full-text SMR articles on publicly accessible internet sites is prohibited. To obtain permission to post articles on secure and/or password-protected intranet sites, email your request to smr-help@mit.edu.