Pillars of Trust

Methods for managers to avoid losing trust in the digital age
"If you take a broad enough definition of trust, then it would explain basically all the difference between the per capita income of the United States and Somalia”

- Steve Knack, World Bank senior economist with over a decade of expertise in the economics of trust
TRUST EVOLVED FAR BEYOND HANDSHAKE DEALS

In society and in business, trust is critical. It enables business to function and create value. Without it, the opposite happens. Growth slows as faith in institutions, employers, employees, regulators and partners unravels.

For generations, our expectations and markers of trustworthiness evolved. Once, a handshake between two individuals could reassure both parties would follow through on agreed upon terms.

In 20th century India, the Tata name inspired trust in diverse set of products and services and ensured customers that quality would be high and end product would be what was agreed. The whole Tata system relied on maintaining customer trust as the reputation kept new customers coming and existing customers returning.

Modern brands have invested billions of dollars to ensure customer associate their logos and products with quality and integrity.

“Trust bestowed by the consumer can not only make or break a business, it can also ensure you survive a problem in the future.”

- Vanessa Mitchell, CMO, IDG

In an age of rapid change, the symbols and expectations of trust are transforming. New business models, like ones built on the sharing economy, require trust at their core to operate. Long distance business transactions in which the parties don’t know each other’s names are commonplace.

It’s a far cry from handshake deals.
Importance of Trust in the Digital Age

Trust has become one of the defining issues in the digital era. From individual citizen trust scores in China’s Social Credit System to Apple’s cell-phone trust scores to detect fraud, measuring trust and differentiating actions in response is now commonplace. While methods of measuring trust are increasingly accepted, breaches of trust are even more visible and material to corporate reputations and business results.

Trust is also increasingly important to customers, as violation of trust are more frequent and more visible. With declining trust in most American institutions and a never-ending series of headlines about bad actors further eroding trust in business, designing and managing for trust is critical.

54%

Percent of 7000 companies which experienced a significant degradation of customer trust according to a 2018 Accenture study

180B

Aggregate lost revenue from companies that experienced a significant degradation of customer trust in the same 2018 Accenture study.
In today’s business environment, breaches of trust are questions of when, not if. Every business model and each business decision contain some risk of precipitating a trust event. While there are situations in which destroying trust is unforeseeable, most trust-degrading events are predictable, proactively controllable, and ultimately preventable.

Too many companies are needlessly damaging customer, employee, supplier, investor, regulatory or simply general public trust. To win in a trust-scarce world, managers must actively prioritize building trust into every aspect of their operations and culture.

Although some actions that degrade trust will continue to be unanticipated, managers can take proactive action immediately to ensure their organizations are designing for trust from the start and well prepared to recover from breaches.

To help managers avoid losing trust in the digital age, we developed five pillars to guide decision making and internal processes. The pillars are transparency, communication, access, culture, and business model risk.

In the following pages we provide case studies of companies and situations where each of these pillars have been managed well or poorly. By leveraging the five pillars in the course of everyday work, managers will be more likely to avoid preventable breaches of customer trust.
At its core, organizations that prioritize trust must embrace transparency. Transparency enables stakeholders to better understand a company’s operations, reassuring customers of the integrity of the company’s processes and controls. Trust in a company increases with greater transparency.

When material information is withheld, stakeholders feel misled and deceived, diminishing trust in the company and its products. Failing to disclose information to consumers has cost companies in fines, reputation damage and stricter regulatory oversight.

**CASE STUDY: NEST SECURITY SYSTEMS**

Nest Security System, owned by Google, failed to disclose a microphone included inside the product but never listed in the device’s specs, leading to massive outcry and Congressional investigation. With over one-third of consumers owning smart home devices, Google’s blunder was not including a microphone in the Nest system, but instead not disclosing its existence and letting customers live with unknown microphones in their homes. As a result of the failure to disclose, the Senate Commerce Committee demanded written answers and an in-person briefing from Google CEO.

**CASE STUDY: BLOCKCHAIN**

The emergence of Blockchain, frequently heralded as the institutionalization of trust, more accurately indicates the complete disappearance of trust. The transparent nature of a Blockchain ledger absolves the need of trust in a system, instead relying on complete transparency. Some of the hype surrounding Blockchain applications is driven by the rising level of distrust and lack of transparency in existing systems for high-value transactions that require high integrity.
COMMUNICATION

Managers must communicate clearly and simply with all stakeholders. Regardless of stakeholder group, people want to be informed about what the company is doing, where it is going and how they will be impacted.

Communicating regularly and simply is an easy way for managers to develop trust and create stakeholder loyalty while preventing public backlash.

CASE STUDY: FONTERRA

As part of their growth efforts, New Zealand dairy company Fonterra expanded into China. In 2013, in response to a warning about a possible contaminant in their Chinese supply chain, the company immediately faced a deluge of negative press and online comments. Instead of a standard press release, Fonterra created a credibility-rebranding campaign in less than a week and had employees use social media to respond, correct misinformation and build personal connections with the concerned customers (and increasing positive comments by 1,500%). A few weeks later Fonterra launched a premium dairy product and it promptly sold out, as a result of their amplified communication strategy.

CASE STUDY: USER AGREEMENTS

The average user agreement for a cell phone app takes 45 mins to read at a 12th grade reading level. With the average person installing 60 - 90 apps, the burden of time to read and understand each app is high. GDPR requirements to simplify language and streamline time required to understand will push app providers to communicate with customers in a more user friendly and accessible manner. Had app providers taken the proactive steps to more clearly communicate their terms of service, legislation might not have been necessary to force their hand.
ACCESS

Who can control accounts, manager features and access varying levels of data will inevitably evolve as a business grows. However, it is important to establish criteria and carefully limit access to sensitive materials and controls that could be tampered with or used improperly. Ongoing monitoring and access accountability must be an ongoing process.

CASE STUDY: DATA ACCESS AT TWITTER

In 2017, President Trump’s Twitter account was taken down by a rogue contractor on his last day. For members of two customer-facing teams, accounts could be shut down as simply with ‘one click’ by a Twitter team member, regardless of account owner. The episode demonstrated how Twitter’s efforts to combat harassment and the spread of misleading information created access and controls vulnerabilities allowing bad employee actors to disproportionately impact the company’s reputation and public trust in the integrity of its platform.

CASE STUDY: PARTNER DATA ACCESS AT FACEBOOK

Prioritizing growth above all, Facebook repeatedly did not monitor or responsibly control the extent to which partners could access users’ data. Netflix and Spotify repeatedly found that they had complete access to customers messages, and a former employee reported “It was chaos. There was no set of principles that says this is how we do things and how we do not do things. They would forget to shut things down, literally for years.” The nonchalance that characterized Facebook’s approach to managing data that led to the Cambridge Analytica scandal contributed a 66% decline in user trust of Facebook.
CULTURE

Company culture is key in creating an environment for trust to foster between teammates and to maintain trust with internal and external customers. Culture helps create a proactive ethos to define and hold the company accountable for its trustworthiness.

CASE STUDY: UBER

Uber famously highlights the short-term and long-term impacts of a toxic culture impeding trust. The company’s growth-at-any-cost mindset, without regard for customer or driver trust, resulted in several egregious trust-busting incidents. These incidents -- the cover-up of a hacking breach that impacted over 57 million customers and 600,000 drivers, Project Greyball, a law enforcement avoidance program, plus rampant reports of sexual harassment, a U.S. D.O.J investigation into managers violating laws against bribing foreign officials, trade secrets theft from Google and more -- show a company-wide cultural disregard considering potential loss of trust impacts from company actions.

A cg24 report estimated that Uber had $696 million of revenue at risk following the #DeleteUber campaign and that while short-term switching was low, their main competitor directly benefited from increased market share as Uber’s brand image took a bigger hit than expected and Lyft “seized the opportunity to brand itself as a more socially conscious alternative.”

The long term impacts are still unfolding. Uber’s IPO filing acknowledged, “Our workplace culture also created a lack of transparency internally, which has resulted in siloed teams that lack coordination and knowledge sharing, causing misalignment and inefficiencies in operational and strategic objectives.” This legacy has also risked one of the key drivers of Uber’s future success: drivers, as it continues to face an uphill battle with driver retention due to a lack of fairness and transparency.

CASE STUDY: HUBSPOT

Hubspot competes against well-entrenched competitors, growing to over a market cap of over $1b in less than years. Leadership contends that their “Culture Code” has been key to any success. Hubspot’s Culture Code provides principles for managers to make tough decisions, even forgoing short term revenue in order to maintain customer trust in the long term. They take transparency seriously. Everyone at the company has access financials, board meeting notes and management meeting notes. They have also been recognized by their employees, as in 2018, Hubspot was named Business Insider’s #3 tech company to work for.
BUSINESS MODEL RISK

Managers must constantly monitor and manage the risk embedded in their company’s business model and value drivers. If company business models are driven by generating and monetizing user data, driving usage, and integration into user’s day-to-day life, unintended risks arise driven by optimizing for key business metrics that incentivize bad company, employee, or use behavior.

CASE STUDY: SNAPCHAT SPEED FILTER

In 2017, Snapchat released a feature allowing users to capture and share their date and time, temperature and speed. This feature resulted in serious unintended consequences. Young adults across the country recorded themselves accelerating well above 100 miles per hour, several precipitating fatal car crashes.

Snapchat’s speed filter built in incentives for bad user behavior. The company failed to recognize and manage the risk, resulting in loss of life, reputation damage and costly lawsuits all which could have been avoided by proactively assessing how the new feature would encourage bad behavior.

CASE STUDY: GOOGLE USER DATA

Following a year of heightened public awareness over lack of personal data control and mounting backlash, Google recently announced a new feature to allow users to automatically delete browsing history and location data every three or eighteen months.

Responding to user feedback requesting easier ways to manage and control personal data, Google’s actions reveal an attempt to balance the demands for greater privacy and user-control with the utility of Google products personalized by user data.
Strong Security Infrastructure is Foundation for Trust

Strong security infrastructure is table stakes for any company, especially those with sensitive data from email addresses to employee information, from credit card processing to any customer data collection or data storage. Every company must be vigilant with the technology, processes and the workforce training required to protect against bad actors that threaten to erode consumer trust in a company.

Historically, companies focused on perimeter defense to keep bad actors out of networks. However, a series of data breaches in organizations like Experian, Home Depot, Target, and Office of Personnel Management impacted millions of consumers and employees and demonstrated that a perimeter strategy is no longer effective.

Just as issues of broken trust are almost certain to arise, so too are security breaches in corporate networks. New security system focus on defending the perimeter and detecting fraudulent activity within the network. Now the emphasis is on strengthening defenses to stop preventable breaches and preparing to detect and terminate hostile activity.
Businesses also have to contend with their intentional or unintentional impact on the public. Historically, the early days of "cyberspace" were heralded as being a space beyond institutions.

“The most significant impact of the spread of communication technologies will be the way they help reallocate the concentration of power away from states and institutions and transfer it to individuals.”

State Department Staffer Jared Cohen and former Google CEO Eric Schmidt

They meant this to be a positive, however, it has proven to be far more complicated.

In Myanmar, the military operatives used Facebook to spread anti-Rohingya propaganda for years.

This tactic has also been used by state-backed Russians and Iranians and in the United States to spread divisive and “inflammatory” messages. However, in Myanmar the platform was used to incite a genocide. ISIS has also been known to use the platform to communicate and recruit.

Incendiary and harmful content is not limited to Facebook. Youtube and other platforms also have inherent trust risks. Content from cat videos to influencer updates can go viral, as can revenge pornography or concerning self-harm encouragement videos like the “MOMO Challenge.” Hoax or real, the MOMO challenge raises additional questions about trust between users and trust in platforms to keep users safe.

Managers need to recognize any decision or product’s potential to destroy trust via serious public harm.
Managers who effectively learn to manage trust...

**DO:**

1. **DEVELOP PRINCIPLES OF TRUST**
   Develop principles of trust which include ethical guidance and are transparent, accountable and company-wide (ideal) or team-wide (less ideal).

2. **COMMUNICATE & LISTEN**
   Convey the importance of trust to all stakeholders. Listen to customer, employees and stakeholder feedback to inform operations and roadmaps.

3. **ASK "SHOULD I?" JUST AS MUCH AS "CAN I?"**
   Consider ethical ramifications and unexpected user behaviors just as much as feasibility when creating new products.

4. **UNDERSTAND RISK**
   Recognize there will be unpredictable missteps, but account for business model risk in decision-making process.

5. **RESPOND QUICKLY**
   Be prepared to quickly respond to unexpected consequences and blow back.

6. **PRIORITIZE LONG-TERM RELATIONSHIPS**
   Consider long-term customer relationships. Make trade offs that may be painful in the short-term but are beneficial in the long-run.

**DO NOT:**

1. **DEFAULT TO OPEN ACCESS**
   Don’t over-privilege the desire to “act quickly” without understanding potential long term risks and vulnerabilities, especially with external partners and front-line employees.

2. **DELAY**
   When issues of trust, act immediately.

3. **IGNORE**
   Don’t ignore possible misuse or fringe unintended consequences of your product’s intended use.

4. **DEFLECT**
   When user trust is violated, admit the failing and commit to fixing the issue.