accenture

Strategy | Consulting | Digital | Technology | Operations

Trend 5

Digital Trust: Strengthening customer relationships through ethics and security

High performance. Delivered.

Trend 5

Digital Trust: Strengthening customer relationships through ethics and security

Trust is the cornerstone of the digital economy. Without it, digital businesses cannot use and share the data that underpins their operations.

To gain the trust of individuals, ecosystems, and regulators in the digital economy, businesses must possess strong security and ethics at each stage of the customer journey. And new products and services must be ethical- and secure-by-design. Businesses that get this right will enjoy such high levels of trust that their customers will look to them as guides for the digital future.

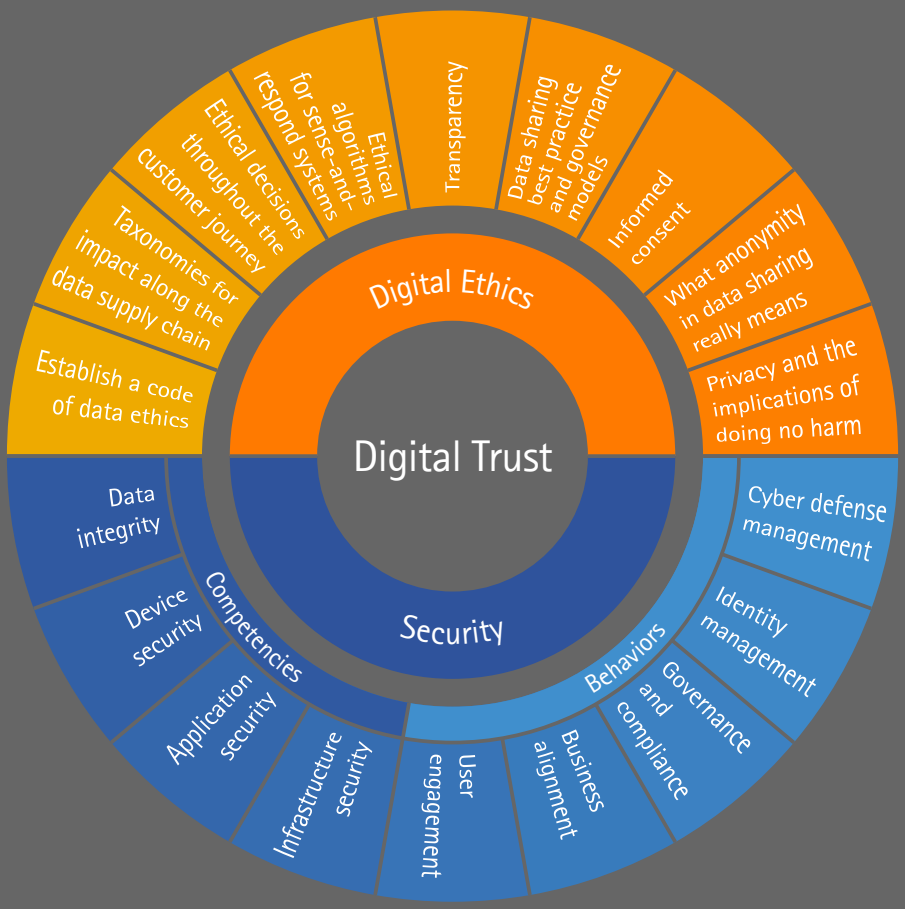
After the consumer outcry from its iCloud breach in 2014, Apple came to understand afresh the importance of trust. Its efforts to be transparent in how it uses and secures customer data is testimony to the value this leading brand places on trust.[1] Its new platforms, such as Apple Pay and HealthKit, are clear beneficiaries of this trusted-by-design approach because the strong security and ethics that are 'baked in' give customers confidence that their digital footprints are secure and private, easing the transition to and adoption of the Apple ecosystem. This underscores the role trust plays as digitally powered companies look to disrupt their own markets and enter new ones.

As the example of Apple shows, trust differentiates competitors in the digital economy where businesses can reach vastly more people, iterate quicker, and make faster, better decisions than ever before. Eighty-three percent of respondents to the Accenture Technology Vision 2016 Survey agreed that trust is the cornerstone of the digital economy. But what's at stake is more than just the benefits of building good will. Inherent in a company's use of technology to rapidly scale is the risk of amplifying mistakes.

Rapidly releasing products and services to tens or hundreds of millions of consumers, or sharing data about consumers at that scale, makes exposure to business risk more systemic. This can potentially result in the loss of previously established trust, which in turn can lead to the loss of customers, market share, and company valuation.

83% agree that trust is the cornerstone of the digital economy.

Exemplifying the importance that trust plays in its ability to do business, Apple told a federal court that "forcing Apple to extract data [from mobile devices]...could threaten the trust between Apple and its customers and substantially tarnish the Apple brand."[2] Companies such as Apple that understand the importance of trust in the digital economy know that in order to compete, push boundaries, and offer new services, they must design products and services that are both ethical- and secure-by-design. Microsoft is designing products this way too. The company is opening data centers in Germany that will be managed and operated by a third party, allowing German customers to use Microsoft technology but to have all of their data controlled by a German company, without a 'back door' for Microsoft.[3]



By building new offerings in such a way, companies are building trust and minimizing systemic risk. This is critical, especially where data is needed to inform personalized services at scale, using technologies that require troves of personally identifiable information (PII). As data-centric products and services put data-handling concerns in the spotlight, 82 percent of executives agree that companies are exposed to exponentially more risk. Managing that risk and building trust starts with data ethics and security.

Recognition of new risks from digital transformations has already propelled security investments across all industries. Global information security spend is set to exceed US$100 billion by 2019, according to Gartner.[4] Even so, a singular focus on security is insufficient to account for the risks encountered by digital businesses.

Over 80 percent of companies are required to comply with data-handling protocols that go beyond their internal controls. To account for these intrinsic risks in other parts of a digital business's operations, data ethics—and, more comprehensively, digital ethics—are critical.

Although consideration of ethics should be a key part of digital transformations, it's a new area of focus for the majority of businesses. It's not just customers who are sounding the alarm: 80 percent of knowledge workers are demanding stronger ethical controls on data too. Currently, most companies' strategies align to a single vector: privacy, which is just one component of data ethics. Digital ethics is even broader, encompassing the operational processes where data is applied to affect real-world outcomes.

Data Ethics vs. Digital Ethics:

Data Ethics—moral governance of the integrity, handling, control, and provenance of data.

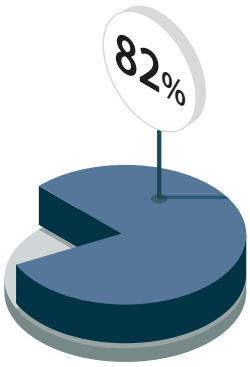
Digital Ethics—data ethics and moral governance of actions taken as a result of insights derived from the analysis of information (where 'information' is data with context).

Company boards, and their risk committees in particular, need to pay attention. Without comprehensive policies, training, incentives, and consequences for data and digital ethics, exposure to risk increases and adverse outcomes are more likely. Cyber risk insurers recognize this and are now demanding more controls and policies to be in place before underwriting cybersecurity insurance.[5] It's a trend that's set to continue.

New Responsibilities

Businesses must identify an executive responsible for developing governance models, taxonomies, and principles-based codes. This role will also focus on technically challenging areas such as decision-making in autonomous systems and confront today's assumptions of what informed consent is, how to do no harm, and what it means to be truly anonymous. These are no longer philosophical puzzles. They are critical business realities that all companies must solve.

One way to account for this risk is to consider whether trust is being enhanced or eroded at every step of the customer journey. What's more, if companies fail to recognize and 'design-in' strong ethical controls in a way that accounts for cultural variances in governance, and human and technological processes throughout the customer journey, they face further damaging outcomes. Eighty-two percent of survey respondents agree that a lack of security and ethical controls on data could exclude them from participating in others' digital platforms and in broader ecosystems—an increasingly critical go-to-market strategy.



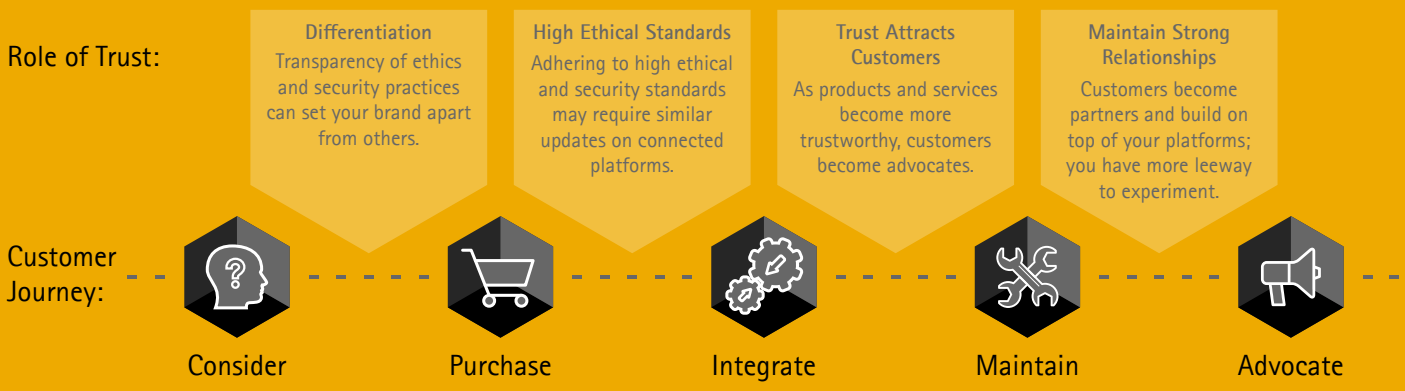
82% say a lack of security and ethical controls on data could exclude them from participating in other companies' digital platforms and broader ecosystems.

Additionally, a failure by companies to address data and digital ethics may prompt regulators to impose their own rules and legal frameworks—and any change in the regulatory environment can not only be onerous, but also contribute to both a stifling of innovation and a forcing of changes in business models. Look at how the invalidation of 'safe harbor' caused scores of companies to redesign how they share PII between the European Union and the United States.

Wherever regulatory scrutiny strikes next, one thing is certain: corporate indifference to data and digital ethics can increase reputational risk and create unwelcome headlines.

Uber's pricing algorithm, based on supply and demand, failed to consider extraordinary circumstances and quadrupled fares during a hostage crisis in Sydney.[6] Facebook experimented with the emotional impact of negative news stories on 700,000 users (violating informed consent).[7] These are two examples among others that have made headlines in the past two years, with some companies facing class-action lawsuits. In these incidences, widely reported public outrage drove the companies to change their data policies.

Trust and the Customer Journey



Making the right decisions internally to gain customer trust is only half the battle; making sure outsiders don't gain unauthorized access to data and abuse hard-won trust is also crucial. That's why next-generation security mechanisms are following the data, taking user behaviors into account, and extending well beyond the perimeter. Wherever data goes, security must go with it. To address this challenge, security solutions—such as security-aware application design, integrated database security, dynamic access controls, and runtime application protection—are being integrated into new products. This data-centric philosophy is also revolutionizing identity and access management. For example, InAuth is a mobile-device security company that establishes the trustworthiness of a device before granting it access to network resources. Once a device is validated, solutions from the likes of BioCatch employ multifactor authentication that considers the way users interact with devices as a way to verify and provide persistent identity.

Global companies are also moving decisively in this direction. AT&T, for example, is undertaking a wholesale upgrade of its back-end architecture, moving toward data-centric security in its databases and its applications. It's doing this to ensure high data integrity, so data is stored securely and not manipulated in transit.[8] Coca-Cola, Verizon, Google, and Mazda are all taking a similar approach.[9] Embracing this transformation, their leaders understand that trust comes from robust security and data ethics.

The scalability enabled through the digital transformation of the customer journey has positive and negative dimensions. The best way to minimize downside risks is to maximize trust. Better security, on its own, won't be enough; nor will rote compliance with privacy regulation. Organizations must manage data and digital ethics as core strategies for mitigating business risks, just as they do with cybersecurity. Their reward? Unprecedented growth in an interconnected, platform economy, with minimal downside risks. Those who master this transformation can move beyond the first level of customer trust, namely that products will meet or exceed expectations, to a higher level where empowered individuals trust a company to lead them into the digital future.

Predictions

Looking into the future, trust and digital ethics will continue to play an increasingly critical role in business operations and become the minimum standard for participating in industry ecosystems.

The Trust Bust: High-profile digital ethics failures will create new governing bodies, new regulations and a new category of jobs.

The CEO Gets a Twin: Trust becomes paramount, and a new leader emerges—the Chief Ethics Officer.

Key Takeaways

- Ethics and security must be primary considerations in any digital transformation.
- Exposure to risk scales in proportion to digital business operations.
- To protect against downside risk, businesses must foster strong ethical decisions, effectively use security to protect against external threats, and build trusting relationships with ecosystem stakeholders.
- In procuring new technologies, security and ethics must be key evaluation criteria.
- Look for opportunities to build trust at every engagement point along the customer journey.

Digital Trust:
100-Day Plan

Over the next three months, businesses should understand the current state of digital risk they're exposed to and benchmark data points that can be improved.

1. Survey stakeholders in an effort to quantify the level of trust across your offering portfolio.

2. Search customer service logs for the word 'trust' and run sentiment analysis against the results to gain understanding in how customers perceive your offerings and brand; make a top-five list of the least trustworthy offerings.

3. Take an inventory of data-driven business processes; describe the current and potential opportunities for enhanced security and data ethics for each.

4. Identify the executive(s) responsible for building and maintaining trust, digital ethics, and security with vendors, partners, and customers.

5. Research what your competitors do to build customer trust. Record what builds and erodes trust. Brainstorm opportunities for improvement within your own operations.

6. Partner with an academic institution, non-profit, or industry group to dive deeper into one aspect of digital ethics. Publish findings/advice for others.

7. Compile a list of opportunities for security to move closer to data.

Digital Trust:
365-Day Plan

In a year, businesses should have started to include provisions for strong digital ethics in their digital transformation strategies, have new security pilots underway, and have concrete plans to mitigate violations of customer trust.

1. From the top-five list of the least trustworthy products, do a complete customer journey analysis and try to understand where opportunities exist to build trust.

2. Discuss hiring a chief digital officer, chief trust officer, or chief ethics officer with your board of directors. This role will be responsible for orchestrating the establishment and maintenance of digital trust.

3. Pick one product/service to maximize trust. Build metrics for tracking improvement over time. Report results to product teams and challenge them to meet aggressive targets.

4. Start tracking metrics for trust and both data and digital ethics. Use this data to include trust and ethical practices in your company's annual CSR report.

5. Implement a portfolio of solutions to move security closer to data. Describe how their implementation has mitigated downside risk. Share this report with your CIO and CFO in an effort to reduce insurance premiums.

References:

Trend 5

[1] "Who Has Your Back? EFF Gives Apple, Adobe, Yahoo, And Dropbox Perfect Scores On Protecting Your Data," Tech Times, June 19, 2015.

[2] "Apple Tells U.S. Judge 'Impossible' to Unlock New iPhones," Reuters, October 20, 2015.

[3] "Microsoft to Open Data Centers in Germany," The Cubic Lane, November 15, 2015.

[4] "Forecast Analysis: Information Security Worldwide, 2Q15 Update," Gartner, September 8, 2015.

[5] "As Cybercrime Proliferates, So Does Demand for Insurance Against It," NPR, October 12, 2015.

[6] "Uber Backtracks After Jacking Up Prices During Sydney Hostage Crisis," The Washington Post, December 15, 2014.

[7] "Everything We Know About Facebook's Secret Mood Manipulation Experiment," The Atlantic, June 28, 2014.

[8] "How AT&T Is Virtualizing Security," WSJ CIO Journal, May 18, 2015.

[9] "Google Moves Its Corporate Applications to the Internet," WSJ CIO Journal, May 11, 2015.

Contacts

For more information

Paul Daugherty
Chief Technology Officer
paul.r.daugherty@accenture.com

Marc Carrel-Billiard
Managing Director,
Accenture Technology R&D
marc.carrel-billiard@accenture.com

Michael J. Biltz
Managing Director,
Accenture Technology Vision
michael.j.biltz@accenture.com

accenture.com/technologyvision
#techvision2016

About Us

About Accenture Technology R&D

The Technology Vision is published each year by Accenture Technology R&D, the dedicated research and development organization within Accenture that includes the Technology Vision group, Accenture Open Innovation and Accenture Technology Labs.

For more than 20 years, Accenture Technology R&D has helped Accenture and its clients convert technology innovation into business results. Our R&D group explores new and emerging technologies to create a vision of how technology will shape the future and shape the next wave of cutting-edge business solutions.

We offer seminars on the Technology Vision, which provide a forum to discuss the trends in greater depth and explore the implications for your organization's business.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 373,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.