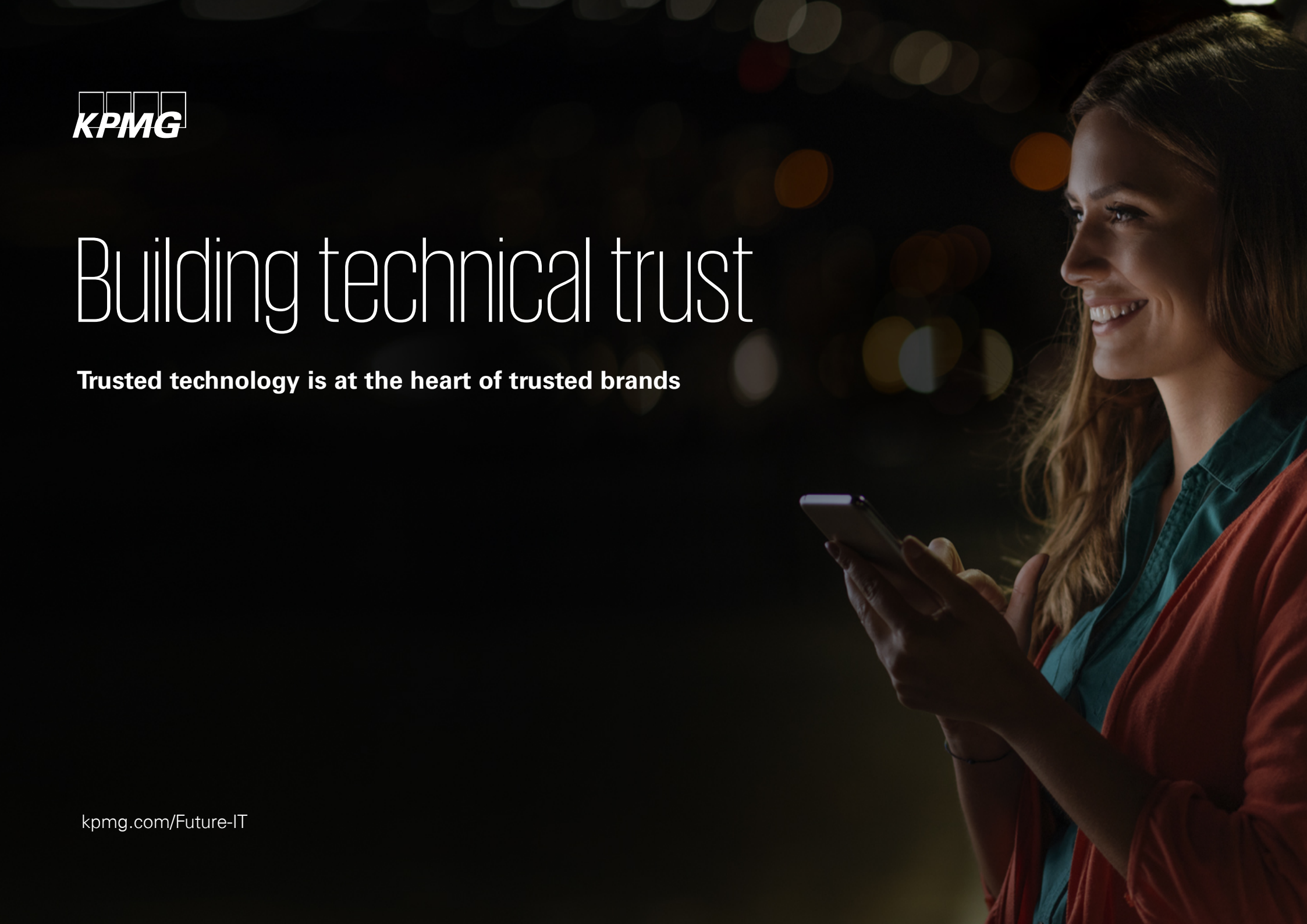


Building technical trust

Trusted technology is at the heart of trusted brands

kpmg.com/Future-IT

Contents

The digital age is raising the stakes on trust

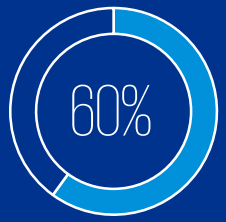
Trust has always been a powerful currency. There are real, tangible benefits for organizations that build customer relationships based on trust. Research shows that trusted brands enjoy increased customer loyalty and greater customer spend while corporate trust problems are really bad for business.

In the digital era, the stakes for building customer trust have been further raised. Customer trust is no longer just table stakes. It's a key differentiator, essential for consumers to adopt new products and services.

Across industries, technology is becoming integral to meeting customer needs and expectations. Many customer interactions with brands are now digital, from trying on jeans in a virtual fitting room to keeping a home comfortable with a smart thermostat. Even customer experiences that don't take place on a website or an app are likely to be significantly influenced by enabling technologies, from a product order arriving just as inventory runs out to an automatic hotel upgrade for a big spender.

Trust by the numbers

Brands face a trust crisis

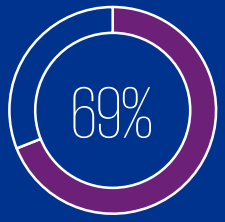


Nearly 6 in 10 customers don't believe companies have their best interests in mind[1]

Distrust is a deal breaker:

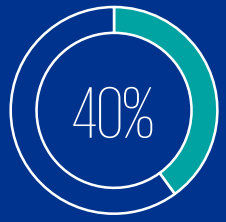
A lack of trust costs global brands $2.5 trillion per year[4]

Values matter



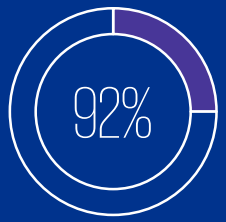
69% of consumers will purchase stock in a company known for its ethical standards[2]

Transparency pays



Nearly 40% of customers would abandon a preferred brand for a more transparent one[3]

Privacy and trust go hand in hand



92% of customers are more likely to trust companies that give them control over the information they share[5]

[1] State of the connected customer (Salesforce, June 2018)

[2] An ethical compass in the automation age (KPMG in the US, 2017)

[3] Trust is as important as price for today's consumer (Inc., May 18, 2018)

[4] Lack of trust costs brands $2.5 million per year (Social Media Week, February 6, 2018)

[5] State of the connected customer (Salesforce, June 2018)

Tech innovation is transforming business, which continues to grow demand for new operating models and trusted platforms.

Worldwide spending forecasts

By 2021:

Cloud services:
$277bn[6]

By 2022:

IoT:
>$1tn[7]

Artificial intelligence:
$77.6bn[8]

Blockchain solutions:
$11.7bn[9]

[6] Worldwide Semiannual Public Cloud Services Spending Guide (IDC, Jan 2018)

[7] Worldwide Semiannual Internet of Things Spending Guide (IDC, Jan 2019)

[8] Worldwide Semiannual Cognitive Artificial Intelligence Systems Spending Guide (IDC, Sept 2018)

[9] Worldwide Semiannual Blockchain Spending Guide (IDC, Jul 2018)

Although technology increasingly underpins profitable customer relationships, 41 percent of organizations do not have a clear digital business vision and strategy, 50 percent do not have a single view of all customer interactions, and 49 percent do not use customer data for personalized experiences.[10] That's poised to change through increased investment in disruptive technologies and new skillsets. In the next three to five years, investment in disruptive technologies like artificial intelligence (AI), Internet of Things (IoT), cloud and blockchain will increase exponentially. As the abilities and applications of new innovations rapidly advance, businesses will embed them deeper into operations. Workforce change will follow: 76 percent of CEOs will prioritize hiring emerging technology specialists.[11] Technology will soon become the backbone of most modern products, services and delivery models.

As technology evolves, technology's influence over customer experience will rise alongside it. Emerging technologies will reshape how customers interact with brands. With the bar set high by the giant technology firms and agile start-ups disrupting nearly every industry, brands will implement innovative technologies throughout the enterprise to deliver customer experiences that are increasingly adaptive, personal, automated, data-driven and transparent.

As this new reality shakes out, technology leaders will face a hard truth. Customer relationship health is becoming more dependent on complex–often invisible–connected technologies. But people instinctively distrust things they can't see, feel or understand.

Many customers are understandably concerned about the risks of doing business in a digital world. Big data helps brands serve customers more personally, but people want control over how their information is used. IoT makes analogue products smart and connected, but also creates very personal data models, additional layers of product complexity, and new cyber threats. AI can create personalized experiences and streamline daily tasks, but it can just as easily be perceived as "creepy" or just add frustration to simple tasks.

Interacting with brands now often requires customers to take a leap of faith. Technology leaders face difficult questions like: "How do we know a machine-learning algorithm will continue to make ethical choices on our behalf?", "Are we certain our car's self-driving system won't malfunction?", "If we hand over our private data to a retailer in exchange for personalized recommendations, who else can access it and how else will it be used?"

As digital becomes the backbone of modern business, the uncertainty that follows is pushing customer trust ever higher on the corporate agenda–and the technology agenda, too.

> **"Customer trust is the number one currency for all new products and services in the digital age. Technology functions that rebuild the operating model to directly promote and sustain customer trust (from norms and behaviors, to processes, policies and governance) will be well positioned for future success."**
>
> Steve Bates, Global Lead - CIO Center of Excellence, KPMG International

[10] Harvey Nash / KPMG CIO Survey 2018 (KPMG International and Harvey Nash, 2018)
[11] KPMG U.S. CEO Outlook Survey 2018 (KPMG in the US, 2018)

The technology risk landscape

32%

of companies say risk management and cybersecurity are the top barriers to technology commercialization.[12] **9%** of CEOs say protecting customer data is a huge concern.[13]

50%

of technology risk leaders say emerging technologies are expanding their scope of work.[14]

33%

one-third or more of companies are rapidly adopting AI, cloud, IoT and mobile without assessing the associated risks.[15]

41%

percent of organizations do not have a clear digital business vision and strategy.[16]

50%

percent of organizations do not have a single view of all customer interactions.[17]

49%

percent of organizations do not use customer data for personalized experiences.[18]

76%

of CEOs will prioritize hiring emerging technology specialists.[19]

[12] The changing landscape of disruptive technologies (KPMG International, 2017)

[13] KPMG U.S. CEO Outlook Survey 2018 (KPMG in the US, 2018)

[14] Disruption is the new norm: Tech risk management survey report (KPMG in the US, 2017)

[15] Disruption is the new norm: Tech risk management survey report (KPMG in the US, 2017)

[16] Harvey Nash/KPMG CIO Survey 2018 (KPMG International and Harvey Nash, 2018)

[17] Harvey Nash/KPMG CIO Survey 2018 (KPMG International and Harvey Nash, 2018)

[18] Harvey Nash/KPMG CIO Survey 2018 (KPMG International and Harvey Nash, 2018)

[19] KPMG U.S. CEO Outlook Survey 2018 (KPMG in the US, 2018)

Technology leaders can be catalysts for customer trust

When technology powers the customer experience, trust must be a key ingredient in a company's digital products and services. In fact, building trust in technology–what we call "**technical trust**" –is now a strategic imperative for technology executives, including the chief information officer, chief technology officer, chief information security officer and chief digital or innovation officer.

Technical trust is a set of enterprise technical attributes that help deliver a positive customer experience–one that is accessible, frictionless, resilient, secure and transparent. Establishing technical trust is foundational to a successful relationship with tomorrow's customer, who wants all the benefits a digital experience can bring, but without all the risks.

Technical trust enables companies to serve and protect customers, superbly and consistently, in the digital age.

When companies achieve a high level of technical trust, they demonstrate command and control over the powerful technologies that shape customer interactions, creating a true competitive advantage. This calms natural fears and uncertainties with bringing technology into our daily lives and drives better outcomes. Customers will feel protected and cared for, and they'll more readily believe in, accept and adopt digitally–enabled products and services. Trust allows a good product to evolve into a sustainable platform rather than sizzle out as a technology fad.

Technical trust can directly influence customers' perception of an organization. Forrester posits that the external sentiment of a company is driven by transparency, integrity and competence, which are customer perceptions formed over time through past interactions.[21]

The concept of technical trust doesn't just apply to customer-facing technologies. It encompasses the full range of operational technologies across the entire business that work together to drive the customer agenda forward. It also helps serve the internal customers (i.e., employees) who are using new technologies and data sources to aide their daily job responsibilities. Employees are more likely to embrace new technology at work–from email platforms to mobility apps to workflow and collaboration tools–if they understand the purpose and can trust the outcomes are better than the previous way of doing things.

As leaders of the technology agenda, technology executives can be catalysts for customer trust by enabling and aligning key capabilities throughout the front, middle and back–office. Trustworthy technology builds trustworthy brands. By establishing technical trust, technology executives can help the organization deliver a lasting, preferred experience to the consumer and realize the substantial business benefits of doing so.

I will serve and protect the customer

Technical trust is a set of enterprise technical attributes that help deliver a positive customer experience.

I believe and trust your brand

Technical trust directly influences customers' **perceived trust**, their overall opinion of an organization's transparency, integrity and competence, formed over time through past interactions.[20]

[20] The mechanics of trust (Forrester, December 2018)
[21] The mechanics of trust (Forrester, December 2018)

Technical trust → **Perceived trust**

Technology executive
Catalyst for trust

Back office
- Enterprise & product security
- Internal products & apps
- Availability & resiliency
- Third–party governance
- IT risk management

Middle office
- Connected supply chain
- Product innovation and engineering
- Data-driven insights & analytics
- Process automation

Front office
- Customer experiences
- Digital channels (mobile, IoT)
- Product, platform & services
- Sales and marketing

External customer

How to build technical trust

How do technology leaders help the business deliver winning–trusted–solutions to customers?

What capabilities should they develop and foster throughout an organization to inspire and uphold customer trust?

Technical trust, an essential precursor to how customers perceive an organization, is shaped by three elements: **serve, protect** and **govern**. Successful technology teams will serve the customer by crafting smooth, dynamic and resilient interactions. They'll **protect** the customer from harm by embedding security and privacy into the core product design, using data ethically and responsibly, and fixing issues quickly and transparently when things go wrong. And, as the connected digital ecosystem evolves fast and relentlessly, they'll **govern** the technology with policies and practices that flex with change, ensuring IT continually manages risks that could potentially damage customer trust.

It's also important to remember that this challenge is not just a technical one. Meeting the new strategic mandate to push the customer agenda forward will require the technology organization to transform, shifting its mind-set from operational support to customer service and solutions.

Technical trust

Serve

— Everything-as-a-Service
— Service resiliency
— Frictionless experience

Protect

— Security and privacy by design
— Data as an asset
— Dynamic incident response

Govern

— Continuous asset management
— Digital risk management
— Unified compliance

Perceived trust

Transparency

— Promote clarity, not complexity

Integrity

— Stand by authentic values

Competence

— Ability to execute on promises

The mechanics of trust (Forrester, December 2018)

Traditionally, the IT function's primary charge was building and managing the back-office technologies that support a wide variety of business operations. But as the digital era continues to unfold, technology will become increasingly fundamentally important to the experiences of the end customer. People and things will become more connected. The volume of data created and exchanged between business and customers will explode. Customer engagement will happen more through a digital-physical experience and less face-to-face.

To support essential business outcomes, building and managing customer relationships–not back-office tools–will rank higher among technology leaders' responsibilities. But the old way of managing technology projects will not help them meet those responsibilities. Customer trust cannot be created and nurtured by simply delivering products and services, even innovative digital customer-facing initiatives that are fast-tracked into operation. The problem is bigger than that, and it needs a big solution. Technology is no longer about powering the enterprise; it's about fueling the customer experience. Only a broad transformation of enterprise operations, culture and governance, led by IT, can create an environment that makes customers feel safe, protected and valued.

In the following sections, we examine the core capabilities that make up each element of technical trust–the attributes that should be priority areas for digital age technology leaders.

Serve: putting the customer first

Serve

—Everything-as-a-Service

—Service resiliency

—Frictionless experience

Actions speak louder than words. Delivering high–quality digital services to customers sets the tone for all future interactions and builds the foundation for trusted relationships.

Customers want technology-driven experiences that meet their needs and add value, on their terms. The technology function can help enable such experiences by mastering three capabilities: Everything-as-a-Service, service resilience, and frictionless experience.

Everything-as-a-Service

Calling a cab. Buying groceries. Filling a prescription. Browsing TV shows. Cashing a check. Repairing a car. Technology interfaces are fast becoming the preferred way for customers to interact with brands. Across industries, customer engagement is now delivered through a wide assortment of mobile and digital channels, including websites, apps, and connected products.

Wherever they occur, IT is responsible for operationalizing dynamic and rewarding customer interactions over internet networks. Most commonly, IT will rely on the cloud to both operate its digital products and services and continually improve their functionality to respond to changing customer expectations. Cloud computing, such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS), allows businesses to remotely manage customer-facing apps, develop and test new technologies, and store and manage data off-premises, often through integration with third-party providers.

The Everything-as-a-Service model has numerous benefits. It reduces technology assets and the associated costs, while giving IT more flexibility to evolve products and services at market speed. But it also raises questions about resilience and reliability: What if a cloud vendor discontinues a service or goes out of business, for example? As such, an effective Everything-as-a-Service model will include robust policies to effectively integrate third parties and proactively manage risk.

Service resiliency

If an app isn't loading quickly, people will delete it. If a website is down, customers will go elsewhere.

Influenced by disruptors like start-ups and technology firms, who continue to up the game on customer experience, expectations on brands are changing. Today's customers, accustomed to an on-demand culture of immediate gratification, want instant access to the products and services they hold dear. They expect products and services to be readily available, where and when they need them. As such, reliability is a key factor in building customer trust.

The technology function helps deliver reliable products and services by building resilient technology. According to KPMG research, 62 percent of technology leaders say delivering consistent and stable IT performance is a key business issue.[22] These leaders recognize that digital services must work as well (preferably better) as the analogue experience.

Frictionless experience

Customers place great value on their time. They'll remember digital experiences that save them precious seconds. On the flip side, customers stymied by a burdensome authentication process or forced to fumble through an unintuitive interface will probably turn away. Their prior experiences with other brands have shaped their expectations for friction-free products and services.

IT helps deliver intuitive and natural digital experiences by putting the customer at the heart of technology development. Even as companies push products to market at speed, they must take the time to consider user experience.

Customer-centric design of digital products and services will help build trust and ultimately spur adoption and usage. The reward will likely be well worth the effort: customer-centric organizations are 38 percent more likely to report greater profitability than those that are not.[23]

As retail reinvents itself, customer trust is everything.

In the retail industry, digital technology–and the new business models that spring from it–is transforming how customers are served. Retail was once dominated by traditional brick-and-mortar stores. Then came online shopping. Now, the retail business model is evolving into a hybrid of the two, giving customers real options for how they shop. At the same time, leading edge retailers–including non-traditional industry disruptors–are launching innovative services like same-day delivery, curb-side pickup, customized recommendations and interactive mobile apps that are further improving the shopping experience.

It's an exciting time for retailers, full of possibilities –but also of risks. For retailers to compete today and tomorrow, reaching the digital consumer won't be enough. They must serve digital consumers in a way that meets their increasingly high expectations and improves on what came before. Services must be accessible, personal, frictionless and always available. And as recent retail bankruptcies make clear, the stakes couldn't be higher.

[22] Harvey Nash/KPMG CIO Survey 2018 (KPMG International and Harvey Nash, 2018)

[23] Harvey Nash/KPMG CIO Survey 2018 (KPMG International and Harvey Nash, 2018)

Focus on data security helps platform companies expand reach

One of the largest inhibitors of trust is a customer who feels vulnerable. The brands customers consistently gravitate towards are those they feel will do the right thing, provide a quality product, and guard their personal information.

Over the past decade, the well-known dominant global technology firms have grown rapidly and achieved unprecedented reach and influence by building platforms customers can trust and feel safe using. Although recent privacy controversies in the tech industry have breached consumer trust, these organizations have generally set the bar high on how to build secure products, protect customer data, and provide timely responses and resolutions when issues arise.

Protect: safeguarding the customer

Protect

—Security and privacy by design

—Data as an asset

—Dynamic incident response

Safety is an inherent human need, and it extends to the digital world. The best customer experience can quickly erode if the customer feels mistreated or exposed. To build and preserve trust, companies must protect customers.

Organizations can start by building safeguards into the digital platforms customers interact with and by safekeeping the data customers agree to share. Prioritizing security and privacy by design, treating data as an asset, and establishing dynamic incident response are three key technical capabilities that all contribute to protecting the customer.

Security and privacy by design

Every organization that extends its reach to digital customers is becoming a technology company. This newfound widespread connectivity and inherent technological complexity are exposing organizations to emerging threats they may not be equipped to handle. As the value of data continues to increase, cyber attackers will continue to find new, crafty ways to access and expose digital assets. We have recently witnessed largely publicized data breaches that don't even involve a malicious hacker, but rather a perceived unethical use of personal information. Such incidents didn't involve a true theft of data, but rather a breach in trust of how large companies use personal information of their customers. This has fed the growing public concerns about personal privacy, and led to expansive new regulatory requirements, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act.

We live in an age where security and privacy are table stakes for successful customer relationships. As such, today's business environment demands enterprises change the way they design technology. To protect sensitive customer information, developers must build digital products and services with security and privacy embedded from inception.

Implementing security and privacy at the design stage protects the end customer from exposure to a wide variety of risks that could weaken their trust in a brand. It protects the business, too–from the financial, legal, operational and reputational repercussions of rule breaking, noncompliance and public blunders.

And, it's a true cost savings opportunity. It is significantly less expensive to embed security and privacy activities through the development lifecycle than after the fact.

One study found that preventable software errors such as bugs, glitches and security vulnerabilities are responsible for the majority of software failures, which resulted in $1.7 trillion in financial losses in 2017.[24] Another analysis estimates large companies could easily lose millions per month from lost purchases and customers due to avoidable website and e-commerce errors, like slow page uploads, while spending tens of thousands of dollars per month fixing such errors retroactively.[25]

Data as an asset

Data is the new currency of the digital world, and organizations must treat it as the valuable asset it is. When it comes to building customer trust, safeguarding customer data takes on special importance.

Using analytics and automation, customer data–from demographic information to behavioral histories–can unlock untold value, yielding valuable insights for organizations to improve how they serve customers. But customers want some level of control over how their data is used. They're usually willing to share it if it serves their own needs. But they'll take notice if companies ask for data repetitively, request unnecessary information for simple services, use data for unauthorized purposes, don't seem to take basic steps to keep data safe, or aren't transparent about their data policies. Between the new requirements from GDPR and recent public incidents about how customer data is used and monetized, organizations are expected to have formal data governance functions, including policies and procedures for opt in/out, data minimization, approving use-cases, data lifecycle protection, and retention and disposal.

The technology function can help implement data governance programs to protect prized customer data from theft, loss and misuse. It also keeps customers informed about who is using their data and why.

Dynamic incident response

Businesses recognize that cyber incidents are becoming a near certainty. Given the growing complexity and connectivity of today's business environment, protecting the business from cyber incidents jumped further up the boardroom agenda than any other item in an annual KPMG survey.[26]

Customers also understand that not every breach can be avoided, but they are not tolerant when one goes undetected or is covered up. The late admission of cybersecurity failures has recently driven public mistrust of major brands.

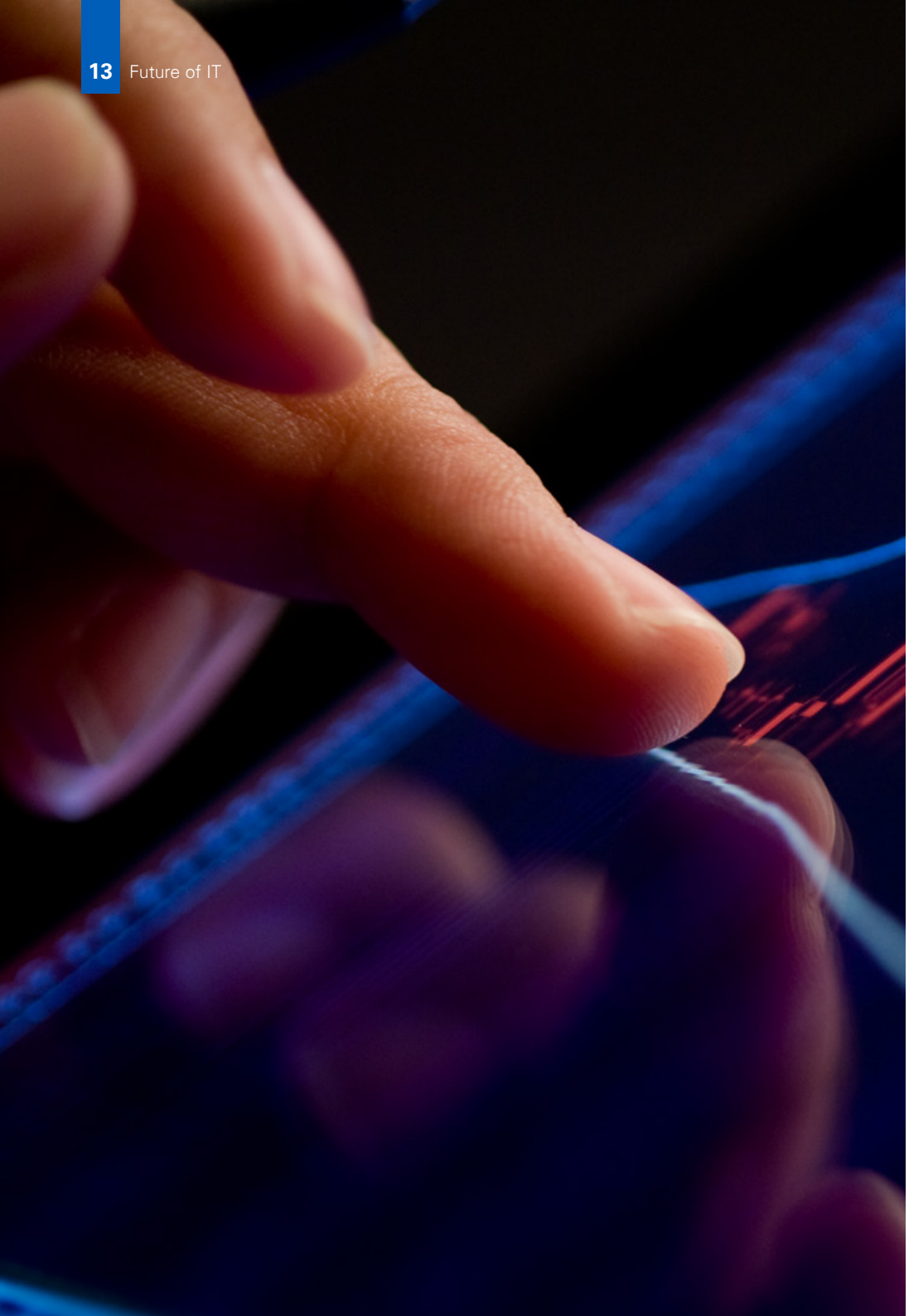
Organizations can help minimize the damage of a cyber breach by viewing incident response as proactive instead of reactive. Implementing layers of defences to harden the technology environment against potential threats is becoming a basic expectation for organizations. Layered defences protect data and systems from interruption, theft, and other malicious actions, and can identify and alert about suspicious activity before it gets too far into the network.

Leading technology functions also invest in predictive capabilities to enable early detection of threats, increase containment capabilities, and reduce incident response efforts and remediation. They ensure breaches are identified quickly and communicated transparently to customers, increasing the likelihood a brand can emerge from a cybersecurity failure largely unscathed.

[24] 2017 Software Fail Watch report (Tricentis.com)

[25] Cost of software errors (Raygun.com)

[26] Harvey Nash/KPMG CIO Survey 2018 (KPMG International and Harvey Nash, 2018)



Govern: managing technology risk

Govern

—Continuous asset management

—Digital risk management

—Unified compliance

The technology behind the products and services that influence such a large part of customers' trust in brands is a constant moving target. As technology advances and evolves, new risks emerge, and the regulatory environment changes and expands in response.

To manage this volatile digital ecosystem, organizations are turning to digital governance. Digital governance isn't bureaucratic and it doesn't slow things down. Rather, it brings people together under a common vision, with shared tools and platforms for creating and managing digital products and services.

Digital governance programs consisting of three key practices–continuous asset management, digital risk management and unified compliance–helps minimize red tape that may limit innovation and sustain responsible growth.

Continuous asset management

The definition of a technology asset is changing in the digital age. While most IT assets were once physical devices residing within an enterprise data center, modern digital products and services are blurring and breaking those boundaries. Hardware, software and data assets may exist well beyond enterprise firewalls.

Having a means to track and monitor these assets is a foundational element for numerous capabilities that drive customer trust, including business resiliency, cyber threat intelligence and response, meeting data privacy regulations, delivering efficient operations and having a positive impact on business outcomes. Technology tools should be utilized to provide real-time identification and profiling of new assets that connect to the network, while enforcing standard security requirements prior to giving a new asset access to any resources.

Digital risk management

Serving and protecting the customer in a way that supports trust-based relationships requires companies to identify and mitigate technology risks that might impair customer trust. The most effective way to do this it to integrate risk identification and mitigation strategies into a common framework aligned with business priorities.

A common, cross-functional digital risk management framework helps establish the strong foundation companies need to measure and manage risk consistently, while also supporting the ongoing growth of digital products and services. It's also forward-looking and adoptive to new technologies, assisting with understanding and navigating risks as they emerge and before they become a problem.

Emerging technologies, like blockchain and intelligent automation, can help introduce innovation into risk management by reducing inherent risks and saving resource time. Blockchain can enable immunity and transparency in digital transactions to create a trusted record verified through consensus. Intelligent automation can help provide continuous monitoring of higher-risk process areas, and data can be leveraged for predictive risk analysis.

Unified compliance

For technology-centric organizations, growing compliance requirements pose a significant challenge. They put stress on personnel and create hidden costs, and they are creating audit fatigue for the business. Many digital products increase the compliance burden by collecting and processing sensitive data. Consider that the GDPR, the new, sweeping data protection law that impacts more than two-thirds of companies, exposes noncompliant companies to fines of up to 20 million euros or 4 percent of global annual revenue.[27] Other compliance requirements that impact customer data collection and processing include SOC 2, HITRUST, ISO27001, and PCI.

Given the growing number of requirements, these compliance initiatives should not be addressed separately or in isolation. Technology leaders should integrate compliance initiatives into a unified program that helps drive better products, aligns audit requirements, promotes control standardization, limits personnel touch points, and reduces redundant information requests.

They can also bring value back to functional teams through proactive monitoring of key risk indicators and insightful risk aggregation dashboards. The goal is to streamline compliance activities and build self-sustaining controls in order to give valuable time back to the business and product teams, ultimately better serving the customer.

As technology evolves, technology governance must too.

As interconnected technologies continue to become embedded into nearly every aspect of an organization, achieving process standardization and meeting compliance requirements is an ongoing activity.

Leading organizations are evolving their risk management and enterprise governance functions to keep up with the pace and adapt to the risks introduced by disruptive technology. This includes modernizing the way IT assets are deployed and monitored, leveraging rich data sources for performance feedback loops and emerging risk identification, and implementing holistic compliance programs.

These activities not only help reduce risks, but can create value through resource efficiency and process optimization.

[27] Harvey Nash/KPMG CIO Survey 2018 (KPMG International and Harvey Nash, 2018)

Key actions now that can help drive future success

Technical trust is at the heart of trusted brands. Building it is a journey, but it can begin today.

There are five foundational actions that organizations can take now to start changing the cultural norms of the modern technology function to build technical trust. Instilling these actions into daily technology operations will be a key source of competitive advantage for organizations doing business in the digital age.

Actions for today, for tomorrow's successful outcomes

1

Build and operate customer-centric technology solutions.

Aligning the IT delivery model with customer needs requires an enterprise-wide organizational adjustment. Project-based IT organizations are a thing of the past. Teams should be structured to support ongoing customer solutions, and service delivery expectations should be directly tied to customer expectations.

Outcome:
The front-, middle-, and back-office functions have smoothen connectivity and the full organization is focused on the customer. There is less "lag time" between systems, and data models are utilized across lines of business.

2

Invest in disruptive technology to help create competitive advantage, make more insightful decisions, and better manage risks.

Today, manual operations hinder productivity and efficiency while increasing the risk of accidental failure. Capitalize on powerful emerging tools that leverage intelligent automation, artificial intelligence and machine learning to promote smoothen, more data-driven operations.

Outcome:
No, the threat landscape won't get simpler. But advanced technology will turn the peaks into valleys. People working all across the enterprise, at all levels, should make smarter, faster decisions informed by artificial intelligence and machine learning. The organization should have newfound visibility into performance and risk indicators and the ability to act on them more quickly and strategically. Staff can retrain on analytics, allowing them to better utilize data to understand trending and predictive models. Events requiring incident management procedures should decrease, while operational efficiency helps bottom-line profits.

3

Know where valuable data resides at all times, to govern and optimize it.

Our interconnected digital world is powered by data. Organizations need robust data governance programs to help manage, protect, and optimize data insights. Data should be governed throughout its lifecycle, inside and outside the organization. A single fracture of trusted data management through misuse or a data breach could impact the reputation and trust of an entire company.

Outcome:
There will be no "silent data." Data is used completely and transparently, allowing organizations to understand and demonstrate to customers that they are inherently secure. Managing regulatory and compliance requirements are more efficient due to better control and visibility around the data lifecycle. Meanwhile, having a better appreciation for the value of data generates more valuable insights through analytics.

4

Manage risks with agility by embracing *trust by design.*

The importance of dynamically managing risks throughout the project lifecycle has never been more obvious. Between direct-to-consumer technology and agile delivery methods, digital solutions are reaching customers faster than ever. Topics like security and privacy controls can no longer be point-in-time checkpoints. The core principles of trusted technology should be embedded into the core design of digital products and services, which requires providing clear guidelines and accelerators to product teams, having sufficient resources and training models, and measuring and mitigating technology risks throughout the lifecycle.

Outcome:
The customer experience will have less friction than typically caused by late-stage risk mitigation techniques (e.g., poor authentication methods, unintuitive data controls, known software vulnerabilities, etc.). The likelihood of post-market incidents related to technology failures will be reduced, and in turn customers will be more likely to trust their data to your brand.

5

Don't get comfortable with today's technology.

Customer expectations quickly evolve, and what is "good enough" by today's standards will quickly be superseded by new technology. Implementing strong technology governance can help continue to evolve technical trust outcomes. Governance should not be viewed as burdensome red tape, but rather a strategic leadership function–a promoter of collaboration and consistency which offers insightful perspective on managing risks.

Outcome:
The agile adoption of disruptive tools that capitalize on artificial intelligence and machine learning should allow the organization to not only achieve desired business outcomes but also support the development of intrinsically secure products and services. Products and enabling technology set the pace for market demand and stay current (or ahead) of customer expectations. Technology trends are predicted in advance, and innovation is fostered naturally throughout the enterprise.

How KPMG member firms can help

For decades, KPMG member firms have been proud to serve as trusted business advisers. We have helped global organizations design and implement technology that earns the trust of customers. Member firms offer a range of services that can help organizations win and build a loyal customer base by understanding and building the key elements of technical trust.

Customer trust assessments

We can help organizations gather a baseline of trust-focused actions to understand their current technical trust capabilities and maturity. This yields an in-depth view of customer technology risks and threats, and leverages industry expectations along with KPMG professionals' experience to build a custom roadmap to increasing the trust of an organization's digital technology.

Create technical trust

We can help organizations build a new governance and operating model revolving around customer trust, implement or improve specific aspects of a technical trust program, and define technology requirements aligned to customer expectations and ongoing digital transformation initiatives.

Trust transformation

We can help organizations regain trust after challenging incidents and help shift a legacy culture to align with next-generation customer expectations. Trust-based principles and actions help turn technology and innovation initiatives into trusted customer solutions.

Trusted data insights

We can help organizations harness the value within a digital customer solution, which revolves around the data. Data helps enable better insights and decisions, and the modern digital customer brings new opportunities and access to levels of data never before experienced. KPMG technology solutions help identify rich sources of data, value-driven use cases, and KPIs and KRIs to enable better automation and more insightful management decisions.

About the authors

Martin Sokalski

Global Leader for Emerging Technology Risk Services, KPMG International.
Principal, KPMG in the U.S.

T: +1 312-665-4937

E: msokalski@kpmg.com

Martin Sokalski is a global leader for KPMG's Emerging Technology Risk network. He has more than 19 years of advisory experience helping organizations design new (and responsible) digital operating and governance models enabled by innovation and emerging technologies. Martin has advised clients on technology-driven innovation and transformation, risk management, security, governance, compliance, and controls integration.

Mike Krajecki

Director, Digital Risk Solutions for Emerging Technology Risk Services
KPMG in the U.S.

T: +1 312-665-2919

E: mkrajecki@kpmg.com

Mike Krajecki is a director in the U.S. firm's Emerging Technology Risk Services practice. He has more than 10 years of experience helping organizations balance the risk and reward of disruptive technologies, including leading the development of KPMG's Internet of Things (IoT) Risk and Governance service offerings. Mike has executed extensive engagements helping organizations build trust and manage risks related to digital products and services, including connected devices, autonomous vehicles, mobile applications, blockchain technology, cloud platforms, and intelligent automation.

Related reading

This paper is part of KPMG's Future of IT series, exploring the six most important things that market leaders will do in IT over the next five years. For more on the Future of IT and to read other papers in the series, please visit **kpmg.com/Future-IT**.

Contact us

For further information on how KPMG professionals can help your business, please contact us.

Martin Sokalski
Global Leader for Emerging Technology Risk Services, KPMG International. Principal, KPMG in the U.S.
T: +1 312-665-4937
E: msokalski@kpmg.com

kpmg.com/Future-IT

Designed by CREATE | CRT106359