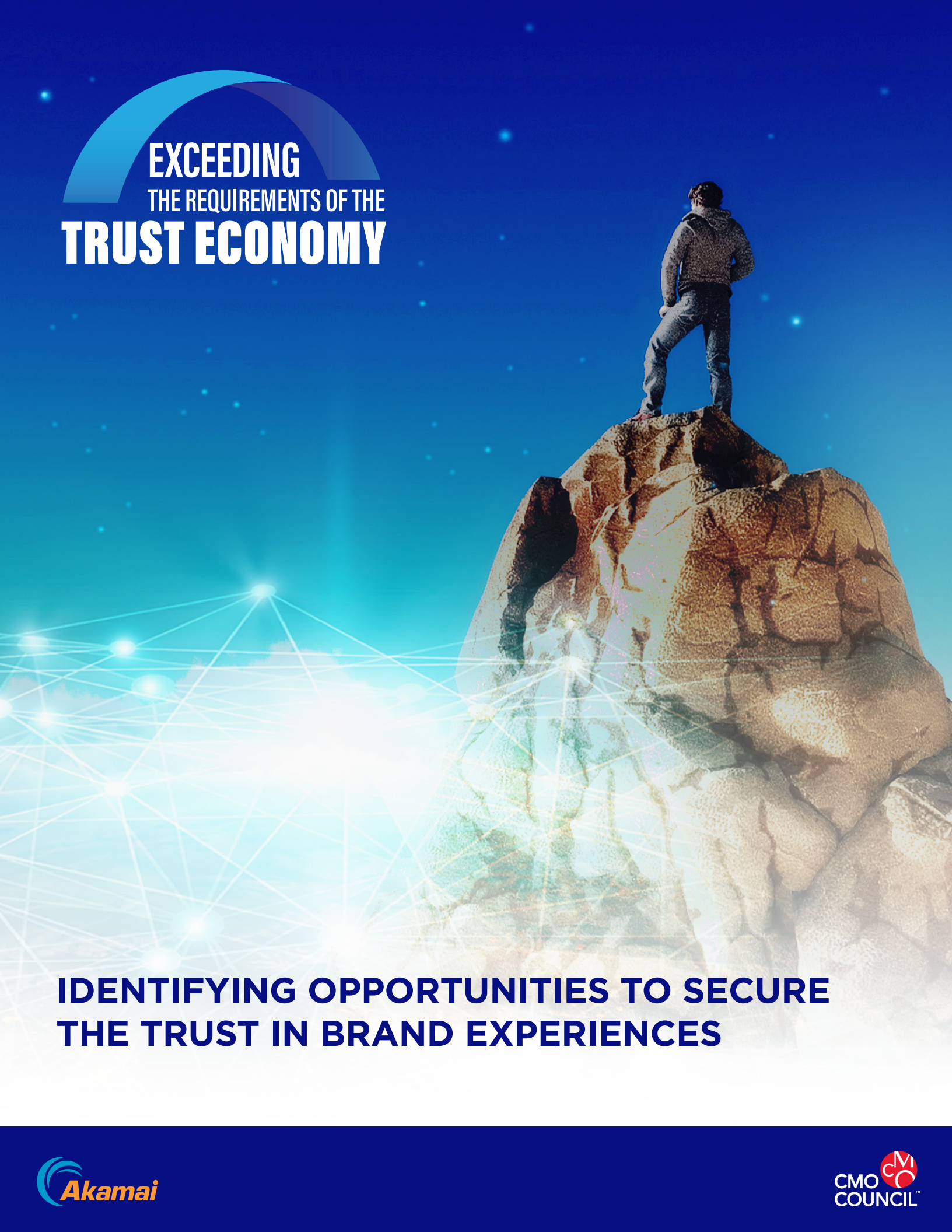
EXCEEDING
THE REQUIREMENTS OF THE
TRUST ECONOMY



IDENTIFYING OPPORTUNITIES TO SECURE THE TRUST IN BRAND EXPERIENCES

Akamai

CMO COUNCIL™

TABLE OF CONTENTS

IS THERE A LINE ITEM OR VALUE ASSIGNED TO TRUST?

According to business analysts and the media, that value is most often summarized as the cost of a data breach of trust, a failure to rise to a promise or a catastrophic incident that hijacks a news cycle. For example, when Target's network security failures resulted in some 40 million credit card numbers and 70 million customer records being stolen, the "cost" of the breach tallied over $320 million after lawsuit settlements, remediation and infrastructure security costs. While $300+ million is a jaw-dropping number, in reality it is really just between two and three percent of annual sales.

In a recent PwC study, 87 percent of consumers said they would take their business elsewhere if they don't trust that a company is handling their data responsibly

The cost less reported is the cost of customer trust lost by the breach: the cost of the Target brand being tied to the word "breach" and the lost perception of trust in the eyes of the customer. Brand reputation monitors tracked consumer perception of Target post-breach as brand trust plummeted some 26 points within a week after the breach announcement to a 10-year low ranking of -9 of BrandIndex's ranking where the high is 100 and the low -100. Ten days after the announcement, the brand's reputation had fallen even further to -19. Despite inducements to revitalize trust that ranged from discounts to free credit monitoring, the brand took months to recover. Analysts projected that the blow to reputation could impact the once $25.5 billion-dollar brand valuation by at least $1 billion.

Warren Buffett said it best: "Trust is like the air we breathe – when it's present, nobody really notices; when it's absent, everybody notices."

The reality is that trust, security and privacy are top of mind for both business and buyer. When the CMO Council asked global marketing leaders what they believed to be the most critical demand of the modern customer, 57 percent pointed to data security, privacy and accountability. This demand is accelerating as customers expect personalization across their brand experiences, from being treated like a known and valued customer to receiving highly relevant and contextual recommendations.

> *Trust is like the air we breathe – when it's present, nobody really notices; when it's absent, everybody notices.*
>
> —Warren Buffett, CEO of Berkshire Hathaway

As expectations increase, so does the risk should those expectations not be met. In a **recent PwC study**, 87 percent of consumers said they would take their business elsewhere if they don't trust that a company is handling their data responsibly. Consumers also understand that their data is a currency for which they can set the exchange rate, as 88 percent indicate that the extent of their willingness to share personal information with a company is directly tied to how much they trust that company.

This elevates a new question the modern Chief Marketing Officer must ask: Is security on the strategic agenda or is it a functional IT task? If it IS a strategic imperative directly tied to the ability to optimize profitable and rewarding customer experiences, how will the CMO adopt the mantle of Champion of Trust?

OUTLINING AND UNDERSTANDING THE EXPECTATION

Customers across the buyer spectrum have become far more aware. They are aware there is a relationship being built, cumulatively over time, between them and the brands they want to do business with. Customers expect to connect, both literally and esoterically. They expect quality services and points of connection and service. They expect products that deliver on their expectations. They expect to be treated a certain way – like busy buyers who just want to be in and out with their purchase, like long-standing customers who want recognition, like a new buyer in need of some wooing and convincing – and that "way" is solely dependent on the customer's context and need.

"What customers are expecting is that we make a really great product… when they come to us and hand us their money, they expect to get what they believe they bought," notes Charlie Cole, global chief e-commerce officer at Samsonite. "While it is fair to assume that this customer has an expectation that we keep their data private, it isn't really top of

mind. When you turn over your credit card at lunch, as you bite into your salad, you are not actively thinking how glad you are this place secures your data."

But, as Cole explains, it is reasonable, and ultimately responsible for any organization to look beyond that initial expectation of product quality, price or even service and respect that even though privacy, security and even compliance are not top of mind, respect and trust continue to be part of the customer equation. There is an explicit assumption that the data being provided is being treated with respect and handled with the utmost security.

57 percent of marketers surveyed by the CMO Council said the most critical demand of the modern customer was data security, privacy and accountability

This expectation and demand has become even more difficult to meet in an age of what Ian Talmage, senior vice president, global marketing and general medicine at Bayer Pharmaceuticals, calls the "democratization of knowledge". In an age of digital technology and real-time access to information, knowledge is not just accessible but also supplemented by noise of the "crowd" via social media. "Social media doesn't always deliver balance, but it always delivers attention," explains Talmage. For a customer who was once satisfied with product and confident that the brands they bought were delivering the quality expected for the price, brands are often left to question their trust quotient based on a shifting scale of knowledge blended with rumor and buzz.

"Customers need to trust," says Talmage. "They need to trust the source – that we are delivering excellent products, that we are doing the appropriate research, that we are testing products in an appropriate way and that we are presenting data in a fair and balanced manner."

This leads organizations to balance the trust that is built through product quality and satisfaction with the ongoing relationship-building that adds to the cumulative trust quotient, today being driven by personalization and choice. "Consumers don't only want choice and personalization, they also expect products that are designed just for them and technologies that respond to what they like," notes Grace Dolan, vice president, integrated marketing at Samsung. "Customers want recommendations for content to watch based on their expressed interests. And as marketers, we CAN deliver these experiences customers have chosen to have… but ONLY if our customers trust us and we are transparent in how we handle their personal information."

According to Dolan, this has elevated her own understanding of the role she and the marketing team must play as "worthy stewards" and protectors of the consumers' privacy rights.

REGULATION AS A CATALYST FOR ACTION

For some organizations, the push towards bolstering trust has come at the demand of regulators, being required to adopt data governance, security or transparency policies in the wake of legislation like the Global Data Privacy Regulation (GDPR) from the European Union and the California Consumer Privacy Act. But the evolution of expectations can't be paced by the evolution of legislation. While regulatory realities have raised awareness and understanding of data, data rights and governance demands, customers are still foundationally focused on their immediate needs and expectations.

> *Customers need to trust. They need to trust the source – that we are delivering excellent products, that we are doing the appropriate research, that we're testing products in an appropriate way and that we are presenting data in a fair and balanced manner.*
>
> — Ian Talmage, Senior Vice President, Global Marketing and General Medicine at Bayer Pharmaceuticals

"Sometimes customer expectations are different than what is legally required," explains Cole. So every day, we think about the relationship and the level of trust we have built. We need to go above and beyond. It isn't enough to match customer expectations anymore. We need to start to predict what consumers are going to want and get to that point before they get there."

Sonesh Shah, vice president of marketing and head of digital for Bosch North America, adds to this perspective, noting that "companies right now have an option: start now by trying to build out what brand and user trust means and take the next few months to really put that into practice. OR you can just follow the regulatory trends and rules coming from State X or State Z and just let the compliance team work with marketing, telling the team what they can and cannot do. Option two may be the more typical path. But it won't be that fruitful."

The question, then, is how does the CMO take a more strategic and proactive security posture to champion and support functional partners like the Chief Information Officer and the Chief Information Security Officer? Best practice leaders and influencers point to **five key mantras** that have aided in advancing their own security and trust strategies.

5 KEY MANTRAS:

1. SECURITY IS AN ATTITUDE

If the security and trust conversation is boiled down to a functional task, it becomes easy to hand off the discussion to IT, legal or compliance guidelines and teams. However, business leaders committed to driving trust as a cornerstone of engagement see security as a strategic brand-driven approach around data.

Shah adds that when security and data governance are viewed as a strategic path, the entire organization has the opportunity to promote and market their products and brand from an attitude of trust. "There is an opportunity to build a strategy of trust by giving consumers control of their data, and making it clear to them that you understand the value of their data. Or… you can hand it all off to IT, in which case you are going to get processes and compliance-based or legal-based approaches, but security and trust will not be adopted into the fabric of the culture and into the foundation of what the brand is, what it could be and what it will mean to the customer."

For security experts like John Summers, vice president and chief technology officer at Akamai Technologies, this approach is called "Privacy-Assured Marketing," or the practice of fulfilling the contract of digital trust forged between customer and business. This attitude goes beyond lip-service to security and privacy. It is a strategic guideline for assuring that trust is built into every strategy and engagement, following the lead derived from a single source of customer truth and data, reinforced by responsible action and reaction.

"Fundamentally, customers want brands to treat them as an individual, knowing the value they deliver. In exchange, they will provide data in order to be met as an individual," explains Summers. "But brands are required to be good custodians of that data."

To adopt an attitude of privacy-assured marketing, Summers notes that the first step is an organization-wide commitment to ensuring customer security, including the personal data being shared in voluntary actions through to transactions. "Brands need to make it explicit that they are a privacy-first organization, implementing the proper governance and distribution of data across brands, channels and touchpoints."

For organizations like Cox Media, this best practice has been implemented, serving as a foundation for all business decisions as a matter of strategy. According to Louis Gump, senior vice president and general manager at Cox Media, trust has been a factor from

moment one. But data privacy has become the center of the way the organization thinks as a path to proving they care about the customer.

"I don't think there is a single leader in our company that doesn't think about data and privacy. It is our strategy to do our best to uphold our end of the bargain specific to data privacy and being inherently respectful of the way viewers consume, which then impacts how they experience working with us."

2. A STRONG POSTURE STARTS AT THE TOP

No single role or leader can advance a culture of trust alone. For many, this will mean partnering with critical stakeholders from IT, security, legal and operations in order to fully champion and support critical decisions, investments and processes that must be embraced and adopted across the organization. However, best practice leaders indicate that the commitment to security is best adopted when this vision is espoused from the very top of the organization.

For Cole and the team at Samsonite, the starting point for this culture of security and trust starts with CEO Kyle Gendreau, who Cole admits has always empowered teams to have a trust-forward posture and readily embraces technology and digital transformation. "I am one part of a two-headed hydra made up of myself and our CTO, who is my partner in all things technology," explains Cole. "My job is to call out where data could be a problem or where data could be abused. This goes beyond pointing out what you can or cannot do from a legal or capabilities perspective. It literally boils down to whether we *should* we do it."

This issue became a sticking point as the Samsonite brand considered the utilization of facial recognition and eye-tracking – all technologies being touted as leading-edge customer experience tools in the next evolution of retail. Noting that there was nothing preventing the installation of cameras in-store for the purpose of eye tracking to better understand how a customer shops, browses and moves from product to product, the question had to be asked: Should the technology be implemented?. Was it part of the customer's expected experience? Did it somehow enhance or enrich the trust and the relationship between brand and potential buyer, or, as Cole mused, "Does this just feel a little icky?"

If Cole and his CXO partners did not have the full support from the very top, had he been within a culture that placed *could* ahead of *should*, the answer to the "icky question" might be very different. Yet in this trust-by-design environment, a strong ethos of security coupled with the technological prowess to quickly decide and act has helped follow through on promises on both product and experience.

3. SYSTEMS GET WHAT THEY NEED. EVERYTHING EXTRA IS A VULNERABILITY.

A company can have an exceptional security team that can implement state of the art, advanced and ever-evolving security solutions. But the reality of today and especially tomorrow is that while technology evolves quickly, bad actors, hacks and exploits will evolve even faster. Even the best built wall will eventually have a crack and in the chaos of an ever-expanding engagement landscape, threat surfaces multiply with every engagement. For organizations that view security as a function and trust as a talking point, security will always simply be a matter of basic compliance, unintentionally putting customer trust at risk.

For brands committed to privacy-assured marketing practices, Summers emphasizes the need for the entire organization and the entirety of the organization's technology infrastructure to be governed by a posture of need and requirement, only delivering the data that a system or engagement needs versus spreading security measures too thin and potentially creating vulnerabilities across massive expanses of data and devices.

Dolan also emphasizes the criticality of assessing where and how data will be utilized in keeping with the consumers' expressed wishes and privacy expectations. "Real-time customer insights are oxygen for marketers. Everything happens in real-time today, from social and digital interactions to the connection between a digital experience and a live event… it is all connected and tied together by data and intelligence as it is happening in real-time. For just a moment, just imagine if you sent your friend a text message and it took a month for them to respond. As marketers, we have to operate at the speed of customer expectation with real-time conversations and engagements. But this all depends on the data. As a result, it has become critical that marketers are involved in the conversation around data, including how we remain respectful of the consumer's expectations, how we secure and safeguard insights and how we distribute and utilize them."

Summers advocates that the first step in this process is to establish a primary view of the customer that includes and extends to all parts of the organization. "Different business units tend to scatter customer data across their systems in different islands of personal information scattered across individual functional stacks," he explains. "By not consolidating data, individual systems run the risk of creating accidentally conflicting experiences that can alienate or frustrate the customer."

Once this unified view is established, the business can set proper governance and proper distribution of data across brands, channels and touchpoints, only serving appropriate data to systems authorized to receive and act on that customer data. This data access policy process must be scoped on a by-application basis so that only relevant data and not the entire data set is shared across systems and platforms.

4. TRUST IS PROVEN EVERY DAY, BUT LOST IN A MOMENT

Leading brands are looking at this opportunity to empower the customer as a turning point in their customer experience strategies, using it as an opportunity not just to strengthen security measures, but also to remind customers of the long-standing relationship and respect built over time. It has also opened up opportunities to leverage policies and practices that are purpose-built around trust.

In a highly regulated and mission-critical industry like health and pharmaceutical products, trust is a critical value proposition. At Bayer, trust is a factor that extends far beyond a dynamic between the brand and its customers. It is part of the culture. "Trust isn't just something between the industry and our customers," notes Bayer's Talmage. "Trust has to be built internally. We have to trust our researchers. We must trust management. We trust the financial community to do the right thing. We trust every person across the organization to always make the right decision. For us, internal trust has to be in place in order to build and prove trust externally. It isn't the industry versus everybody else or against regulators or laws or headlines. For us, we must build trust with everybody because everybody is involved in helping people stay well."

Cole expresses a similar belief as the understanding that customer expectations are constantly moving and evolving, every internal voice and partner in security and trust has to have a voice and vision. This extends into how partners and vendors are brought into the organization's stack. "Everybody needs to be happy in this new security and privacy scenario if everyone is going to respect customer privacies and policies across all systems, teams and perspectives. So for us, everybody: legal, IT, marketing… we all have a veto. We each have the right to say that something isn't right for us and why. We have come to trust and be respectful of everyone's opinion."

The value proposition also begins to shift as organizations place more emphasis on privacy, transparency and security. While this value definition can be "nebulous" as Cox's Gump admits, the more an organization leans in to this new normal, the easier to communicate the value a customer receives from a more informed and transparent security and trust

dynamic. Gump is quick to point out that these decisions can sometimes come at a cost, and has admitted that even Cox has had to make some decisions that the added expense into security and trust would payoff in the long run.

"Everybody has to make their trade-offs. However, the more a company starts with a mindset that building trust is important, and then intentionally puts in place the mechanisms to deliver on that trust, the more likely they are to see some real success. We are in a time where power is gravitating increasingly to the end user, meaning that being respectful and observant of where and how a consumer expects to be protected is that much more important in a cross-platform experience."

Across all brand leaders, a single truth emerges: Yes, these are hard process decisions that will require cross-functional teams and support… they may even be decisions that come with uncomfortable conversations and bigger price tags. But, if conversations are NOT being held and new processes, policies and even platforms are NOT being considered, the impact could be catastrophic. The impact could be as big as a headline of a breach, but it could also be as subtle as the erosion of trust that comes from requests being ignored or disrespected.

5. THE COST OF THE FUTURE CANNOT BE CONSUMER TRUST

Just as digital transformation and experience evolution has brought about new and exciting ways to connect and engage, it has also come at a cost. Increasingly, marketers are having to weigh the value of "should," actively asking if something "should" be done just because it "can be" done. This is especially true as new innovations begin to enter enterprise conversations. One example examined by executives interviewed for this paper is the onset of Edge Computing.

For Mo Katibeh, chief marketing officer with AT&T Business, while trust is foundational across the whole of AT&T, it is critically important as the communications giant takes strides for itself and its customers into new innovations and transformations. "Many of our customers are thinking through their own digital transformation. They are looking for new ways to deliver information to their customers. So we are part of that journey in mapping strategies for our customers to establish a more trusted relationship with their customer and end user," explains Katibeh.

"But when it comes to new technologies, edge computing – coupled with 5G – will fundamentally transform our society as we head into the next decade. When you combine the processing power of the cloud in this network-effect era with the data connectivity that 5G will bring to life, then we will truly be in a position to build smart cities and smart factories. It is going

to not just enable an autonomous car, but everything involved with an autonomous driving experience, from the traffic lights to everything in your home. It will change how we live our lives. So, security becomes a front-and-center conversation in what I recently heard someone call the 'post-truth era'. With this new era comes a new responsibility to innovate and evolve security to protect it."

Samsonite's Cole sees a balance between what has now become foundational and how to quickly stay on top of new innovations. He points to the fact that despite what new technologies or trends are heading towards marketers, there is a universal truth that there is still an upfront customer expectation that must be answered, namely the expectation that brands deliver on the expectation of product, value and service first. "Never forget that you need to match your customer expectation with the product you are delivering."

From that starting point, staying ahead of expectations becomes paramount. "Don't underestimate how quickly this is all evolving," warns Cole. "People are starting to be held accountable for big failures. Right now, we might not be fully prepared in a proactive way. But we know that consumers want more personalization. We all want to be having a more back-and-forth conversation. Consumers see the value of having their data out there. They want a dialogue when, in the past, we have delivered a monologue on behalf of the retailer. Yes, we need to stay ahead of the technology and regulatory curves. But don't underestimate the speed and the pace of the customer's expectation evolution."

> *Don't underestimate the speed and the pace of the customer's expectation evolution.*
>
> —Charlie Cole, Global Chief eCommerce Officer at Samsonite

Summers has a similar warning for brands not keeping an eye towards users and their control over their own identities. As more applications and devices connect into a broad array of back-end systems and experiences, a trend is emerging where users will expect a password-less experience powered by authentication capable of recognizing trusted users across digital touchpoints. Summers envisions an experience where usernames and passwords, so often the targets of malicious actors, give way to biometrics – a fingerprint, facial recognition, voice – or recognition of the devices being carried as a means for access and authentication. This password-less reality will demand that brands ask new questions about how mobile applications and websites of the future will operate and connect.

"This will all demand a new way of interacting," notes Summers. "We will all have to adapt over time. But for the end-user, ultimately, it is more secure and more supportive of a privacy-first organization."

CONCLUSION

CMO: THE NEW TRUST CHAMPION

New conversations are being initiated with consumers and customers increasingly willing to share data in exchange for value, personalization and experiences rooted in relationships in lieu of just transactions. This new normal demands a new security, privacy and data champion. Without question, while each leader interviewed agrees the entire organization must be part of this new privacy-assured and protection-prioritized model, there is also consensus that marketing as a function, and specifically the CMO as an executive leader, must be part of the dialogue transforming security from a function to a growth-driving strategy.

Bosch's Shah believes that the CMO makes the most sense to make security and trust a strategic path forward. "I don't think you're going to find a strategic brand-driven approach around user data unless you MAKE it the CMO's responsibility. Until you do that, I think you are going to get functional, regulatory approaches. You are going to get processes that never get adopted into the fabric of the culture and into the foundation of what the brand should be."

For Gump, marketing represents the functional area most accountable for the customer relationship. He notes that while the ties between marketing and IT are critically important, the marketing team needs to take a central role the more and more data, privacy and the sensitivity around customer expectations take the spotlight. "The marketing organization, by necessity, has become more closely tied to the data and more closely attached to privacy as issues like addressability and personalization become more and more exciting and expected."

"It is truly an exciting time to be a Marketer," concludes Gump. "It is time for us to really spread our wings and leverage the data we have been entrusted with. It allows us to move so far beyond our core businesses and explore new areas of opportunity and growth."

EXECUTIVE PERSPECTIVES

JOHN SUMMERS
Vice President and Chief Technology Officer
Akamai

MO KATIBEH
Chief Marketing Officer of AT&T Business
AT&T

IAN TALMAGE
Senior Vice President, Global Marketing, General Medicine
Bayer HealthCare

SONESH SHAH
Vice President of Marketing & Head of Digital
Bosch

LOUIS GUMP
Senior Vice President and General Manager
Cox Media

CHARLIE COLE
Global Chief eCommerce Officer
Samsonite

GRACE DOLAN
Vice President, Marketing
Samsung

PARTNERS & AFFILIATES

ABOUT THE CMO COUNCIL

The Chief Marketing Officer (CMO) Council is dedicated to high-level knowledge exchange, thought leadership and personal relationship building among senior corporate marketing leaders and brand decision-makers across a wide-range of global industries. The CMO Council's 16,000+ members control more than $1 trillion in aggregated annual marketing expenditures and run complex, distributed marketing and sales operations worldwide. In total, the CMO Council and its strategic interest communities include over 65,000 global marketing and sales executives in over 110 countries covering multiple industries, segments and markets. Regional chapters and advisory boards are active in the Americas, Europe, Asia Pacific, Middle East and Africa. The Council's strategic interest groups include the Customer Experience Board, Digital Marketing Performance Center, Brand Inspiration Center, Marketing Supply Chain Institute, GeoBranding Center, and the Coalition to Leverage and Optimize Sales Effectiveness (CLOSE). To learn more, visit **www.cmocouncil.com**.

ABOUT AKAMAI

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access and video delivery solutions is supported by unmatched customer service, analytics and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit **www.akamai.com**.