

The Trust Imperative

As consumers and employees alike pay more and more attention to the business practices and social impact of brands, only businesses that demonstrate authenticity and social responsibility will have a license to operate.



INSIDE ISSUE 6: Trust: The New Currency of Business Fernando Apezteguia, CEO, NTT DATA UK // **Gender Equality — the New Leadership Advantage** Raluca Melnic, CFO, NTT DATA Romania // **How Companies Can Build Trust in Uncertain Times** Shalene Gupta, Research Associate at Harvard Business School and co-author of *The Power of Trust* // **Thriving When the “Authorities” No Longer Know What to Do** Nick Craig, President of the Authentic Leadership Institute and author of *Leading From Purpose* // **And more...**



Hello.

Welcome to the sixth issue of CXO Magazine

Today, organizations are harnessing rapid advances in technology and cutting-edge innovation to enable success in the marketplace. Yet amid the fast-paced drive to meet customer and business goals, leaders are realizing that, in addition to the speed to deliver, there must be a constant, unwavering focus on building and maintaining trust.

While it may seem a simple term to define, trust – and more specifically, creating trust – is often a complex and highly individualized concept, and one that requires a thoughtful and purposeful approach. With the world seeming to spin faster with each passing day, it can be hard to know who or what to trust as we head into tomorrow.

In this issue of CXO Magazine we explore the theme of The Trust Imperative, and shine a spotlight on the indisputable value of trust between organizations and those with whom they interact – customers, employees and society.

As we look at ways to attain trust, it becomes clear that trust grows as we consider varying points of view. NTT DATA continues to partner with our clients across the globe, listening to their unique needs and providing solid footing during this time of advancing technologies and evolving business models. By combining diverse ideas with trailblazing technologies, we establish strong, trusted partnerships based on a mutual understanding of the challenges ahead, the varied and ever-changing needs of society, and a shared commitment to effectively address them.

Equally as important, when thinking about the talent within an organization, it's vital that trust is at the core of those internal relationships as well. Organizations must ensure that current and prospective employees clearly understand organizational values and goals, and the important role that employees play in supporting them. In addition, as team members provide their time and talent, it's critical that they understand – and trust – the organization's commitment to helping them grow their talents and achieve their career goals. Once organizations realize that their employees' diversity of thought and perspective is the creative power that unlocks the real value of technology, they can solve the complex challenges of today and tomorrow while fostering a dynamic and productive workforce.

Trust has distinctive and varying definitions across an organization and among its stakeholders. What evokes trust will often differ from person to person or situation to situation. Organizations that effectively develop and nurture the intricate facets of trust will reap its inherent benefits, including satisfied customers, motivated employees and a society equipped to face tomorrow. Enjoy the read.

Robb Rasmussen
Global CMO, NTT DATA

Issue 6 Contents

- | | | | |
|---|--|--|--|
| <p>6 Trust: The New Currency of Business
By Fernando Apezteguia, CEO, NTT DATA UK</p> <p>12 Why Trust is Stuck in the U-Bend
By John Elkington, Founder & Chief Pollinator at Volans, professor, and author of <i>Green Swans: The Coming Boom in Regenerative Capitalism</i></p> <p>16 How Companies Can Build Trust in Uncertain Times
By Shalene Gupta, Research Associate at Harvard Business School and co-author of <i>The Power of Trust</i></p> <p>21 5 Minutes On... Trust as the Driving Force of Business
With Shalene Gupta, Research Associate at Harvard Business School and co-author of <i>The Power of Trust</i></p> <p>22 Empathy and Trust: The Human Engine in Organizational Performance
By Alex Allwood, CX expert and author of <i>Customer Empathy: A Radical Intervention in Customer Experience Management and Design</i></p> <p>26 The Human Side of Risk
By Edmund Tribue, VP Risk & Compliance, & Kim Curley, VP Workforce Readiness Consulting, NTT DATA Services</p> | <p>31 Building Trust in Artificial Intelligence
An NTT DATA white paper</p> <p>32 Ushering in a New Era of Customer Engagement with Digital Twins
By David de Castro Pérez, Innovation Manager, NTT DATA Europe & LATAM</p> <p>37 The CXO Podcast: Purpose Strategy Meets Talent Strategy
With Becky Willan, CEO, Given and Ric Garner
Managing Director - Workforce Readiness Consulting, NTT DATA Services</p> <p>37 The CXO Podcast: Safeguarding Our Digital Lives
With Jake Moore Global Cybersecurity Advisor, ESET and Thomas Nørmark Global Head of AI & Robotics, NTT DATA Business Solutions</p> <p>38 Protecting Data Starts With Good Governance
By Eva-Maria Scheiter, Head of GRC Consulting, NTT DATA DACH</p> <p>43 Disruption, Trust and Value in the Fishing Industry
With Ronald Aroca CEO, Tecopesca</p> <p>44 Nurturing Inclusivity and Productivity in a Hybrid World
By Pragya Limbu, Principal Consultant, Business Consulting, NTT DATA UK</p> | <p>50 Thriving When the "Authorities" No Longer Know What to Do
By Nick Craig, President of Authentic Leadership Institute and author of <i>Leading from Purpose</i></p> <p>54 Trusting the Human in Our Future
By Philipp Kristian, Human Futurist, author of <i>The Trust Economy</i> and <i>RESET</i></p> <p>59 5 Minutes On... Building Technology Around Human Needs for Trust
With Philipp Kristian, Human Futurist, author of <i>The Trust Economy</i> and <i>RESET</i></p> <p>60 The Purpose-Driven Corporate: Reimagining the Power of Business
By Debbie Haski-Leventhal, CSR expert, professor of management at Macquarie Business School and author of <i>Strategic CSR: A Holistic Approach to Responsible and Sustainable Business</i></p> <p>64 People-Centric Banking: How to Gain the Trust of Future Generations Through Sustainability
By Gianluca Randazzo, Head of Sustainability, Banca Mediolanum</p> <p>68 Digital Trust: The Difference Between Future-Fit and Obsolete
By Noel Chinokwetu, Security Consulting Senior Manager, NTT DATA UK and</p> | <p>Charanpreet Aulakh, Senior Cybersecurity Consultant, NTT DATA UK</p> <p>72 Earning Trust and Customer Capital Through Integrity
By Ilenia Vidili, Customer centricity advisor, keynote speaker and author of <i>Journey to Centricity</i></p> <p>77 Ethic Zero Trust: Your Digital Transformation Requires a Risk Transformation
An NTT DATA white paper</p> <p>78 Ethics: A Consultant's Guide
By Ian Bower, Director, Business Design Lead, NTT DATA UK</p> <p>84 Elevating Organizational Performance With Design Thinking
By Giselle Chajin Florez, UX and Service Design Lead, Tangity</p> <p>87 5 Minutes On... Authentic Leadership
With Nick Craig, President of Authentic Leadership Institute and author of <i>Leading From Purpose</i></p> <p>88 How Customer Empathy Drives a Successful Omnichannel Strategy
By Daniele D'Aquino, Senior Engagement Manager, NTT DATA Italia</p> |
|---|--|--|--|

Issue 6 Contents

- 93 5 Minutes On... Engagement Strategies to Attract and Retain the Right Talent**
With Ric Garner, Managing Director, Future of Work Consulting Practice, NTT DATA Services
- 94 Technology, Ethics and Customer Trust**
By Vincenzo Iucci, Director, Security, NTT DATA Italia
- 98 The Value of Trust in Business Relationships**
By Claudia Jandl, Senior Cybersecurity Consultant, NTT DATA UK
- 104 Lessons From the Past to Guide the Future: Humanity in Cybersecurity**
By Ortwin Maier, Head of Cybersecurity, NTT DATA Romania
- 108 Future Fit: Implementing Cloud-Based ERP the Right Way**
By Ulrich Kreitz, Head of Managed Services Germany, NTT DATA Business Solutions
- 112 Cybersecurity is Everyone's Job**
By Alexis Martín García, Cybersecurity Analyst, NTT DATA EMEAL & Marcos Búrdalo Romero, Cybersecurity Analyst, NTT DATA EMEAL
- 116 Trust or Bust – Why Transparency Matters**
By Lisa Woodley, VP and General Manager - Northeast, Nexient, an NTT DATA Company
- 121 In Data We Trust: But Do We?**
By Theresa Kushner, Data and Analytics Practice Lead, NTT DATA Services
- 124 Information and Cybersecurity in the UK: The State of Play for Corporates**
Ken Jones, Security Consulting, Regulatory Director, NTT DATA and Warren O'Driscoll, Head of Security Practice, Senior Director, NTT DATA UK
- 127 5 Minutes On... Cybersecurity and Bridges of Trust**
With Martin Stremper, COO, NTT DATA Business Solutions Brazil
- 128 Zero Trust – It Begins With Identity Management**
By Christian Koch, Vice President Cybersecurity and Lead for IoT/OT NTT DATA DACH
- 130 NTT DATA's Zero Trust Journey 1: Blazing the Trail**
By Sushila Nair, Vice President, Security Services, NTT DATA Services
- 133 NTT DATA's Zero Trust Journey 2: Architecture (and What We've Learned)**
By Sushila Nair, Vice President, Security Services, NTT DATA Services
- 136 Make life easy for customers, not for ID fraudsters**
Mickey Nachimovsky, Senior Director, Business Development and Partnerships, NTT DATA UK
- 138 Protecting Customer Accounts and Information in a World of Digital Connectivity**
Edmund Tribue, Risk and Compliance Practice Leader, NTT DATA Services
- 141 5 Minutes On... Customer Experience You Can Trust**
With Alin Cuciureanu, Product Owner MES, NTT DATA Romania
- 142 Tech for Good**
NTT DATA uses its technology and innovation capabilities to help its communities and clients.

Trust: The New Currency of Business

By Fernando Apezteguia, CEO, NTT DATA UK

In a world where skepticism and misinformation have now become the default, trust has become the new currency for business. And those companies that know how to spend it well can create a competitive advantage by making sure that their actions speak louder than words.



“

Trust takes time to build, but can be lost in an instant... While this obviously presents a real threat to organizations with questionable practices, it also creates an immense opportunity.

As modern businesses, we are all on a journey to prove that we can be trusted. This isn't just essential for attracting customers and maintaining their loyalty, but also to win out in the war for talent. Trust forms the basis for a harmonious, mutually beneficial relationship between businesses and society. Trust's value, therefore, is immense – and the difficulty in building and maintaining it is proof of the challenge facing us all today.

For me, a crucial cornerstone of trust is consistency. To be trusted, organizations must not only follow through on what they say, but also be honest when they are not behaving as well as they could (or should) be. Consistency not just of action, but of moral leadership too, is all-important.

Being transparent about less-than-ideal corporate behaviors is challenging, and feels perhaps counterintuitive – after all, the old school of management thinking would recommend building reputation through claiming perfection (or at least, claiming no wrongdoing). But times have changed.

An epidemic of distrust

Across society, doubt and disbelief are growing problems, with once-trusted organizations and authority figures now being regarded with skepticism. In the US, for instance, only 19% of millennials – the largest generation in the nation's workforce – believe other people can be trusted; meanwhile public trust in many institutions is at historic lows.

Several elements have converged to create this current climate of distrust. Social and economic disruption, geo-political tensions and

new technologies all play a part, and citizens and institutions alike are struggling to know where to turn. The latest Edelman Trust Barometer report talks of a “vicious cycle of distrust fueled by a growing lack of faith in media and government”, reflecting the general public opinion that much (if not all) of what we hear reported in the news has a commercial or political agenda.

People also increasingly doubt what they are told by businesses, with 63% of respondents to Edelman's survey worrying that business leaders purposely try to mislead them by saying things they know to be false (or gross exaggerations).

This crisis of trust is hitting close to home. In the UK and Spain, for instance, 79% of consumers say they are increasingly mistrustful of companies, while in France, Canada, Australia, Italy and India that figure is even higher.

Organizations must tread carefully: in our digital age, any mismatch between words and actions is all too easily exposed on social media. Trust takes time to build, but can be lost in an instant – all it takes is reading an exposé of bad corporate behavior. While this obviously presents a real threat to organizations with questionable (or seemingly questionable) practices, it also creates an immense opportunity for those that can demonstrate authenticity and social responsibility.

Acting responsibly attracts consumers. They want to feel they are dealing with organizations that are fundamentally good, and have a purpose and agenda beyond mere self-interest. This shift in consumer attitude is a long way from the Friedman Doctrine of the 1970s, when the economist Milton

“

If your team trusts you, they'll have confidence in your decisions. This confidence in your leadership will see them through uncertain and turbulent times.

Friedman argued that it was the social responsibility of corporations to maximize shareholder returns above everything else. But now, as Simon Sinek put it in his seminal TED Talk, “People don't buy what you do or how you do it, they buy why you do it.”

Trust, and the ability to create and retain it, is fast becoming the currency of successful business – and those who spend it well will see their value rise.

Every crisis is an opportunity

The opportunities to increase business trust are plentiful – and the rewards are great. Companies that are purpose-led, who are champions of privacy and authenticity, and whose behaviors match their words (i.e. high-trust businesses) will be the ones who thrive in a world of increasingly discerning and skeptical customers, employees and investors.

Employees at high-trust companies report less stress, fewer sick days, more engagement and satisfaction – and, all-importantly in today's war for talent, they plan to stay with their employers.

The investment pays off. Organizations on Fortune's 100 Best Companies to Work For, a status that can't be acquired without a high-trust culture, outperform the market by nearly three times.

Talent gravitates towards trust

One of the underlying reasons that high-trust businesses outperform their peers is that talent gravitates toward such organizations. Employees are talking with their feet, leaving workplaces where trust is low. According to research by The Workforce Institute, almost a quarter of employees say they have left a company largely because they did not feel trusted.

As we all know, trust has been tested as never before over the last couple of years by the shift to working from home, driven by the pandemic. Not having direct oversight of employees was a difficult ask for businesses that regarded employee input (being at their desk in a centralized workplace) as more important than employee output (how productive they were).

And while the hybrid working model is now established, some organizations have struggled to put trust first, and instead have turned to ‘bossware’ – productivity monitoring software that tracks an employee's online activity – to ensure their workers aren't shirking. American business news channel CNBC reported that interest in one such product, Prodoscore, leapt by 600% in the second quarter of 2020 as countries began to institute lockdowns. That doesn't seem very trusting.

But trust is reciprocal: leaders can (and must) demonstrate their trustworthiness first, which can be done, for example, through:

- Showing dependability by following through (doing what you say you'll do)
- Showing empathy by treating setbacks as learning opportunities and owning up to mistakes (supporting the individuals on your team)
- Showing respect by creating a diverse and inclusive environment (listening to all perspectives).

If your team trusts you, they'll have confidence in your decisions. This confidence in your leadership will see them through uncertain and turbulent times. The same can be said of the relationship with

“

We are going to have to think differently about trust – not just because it is what consumers want, but because it is the only way that emerging business models can operate.

consumers.

In fact, the employee experience is now becoming a differentiator for consumers as well as staff: a recent HBR article reported that a key element that establishes trust between consumers and companies – alongside ethical business practices, admitting mistakes quickly and honestly, and data protection and cybersecurity – is treating employees well.

New business models will demand trust

Whether an organization has a ‘trust agenda’ will depend very much on the leadership team and their determination to make it part of its culture and vision.

Those that embrace trust will place new emphasis on areas such as acting empathetically, being transparent in all deals, recognizing the need for social accountability, acting with integrity, and ensuring that the fundamentals of modern business, such as data security, are given the highest priority. But we are, I think, going to have to think differently about trust – not just because it is what consumers want, but because it is the only way that emerging business models can operate.

Let’s look for a moment at the rise of the anything-as-a-service (XaaS) model where, rather than buying products upfront, customers pay for them through a subscription model that may be based on access or pay-per-use. We’re probably quite used to this in the consumer sector, but it’s now happening in areas such as industrial equipment. Such models depend on trust because the supplier of an asset needs to effectively guarantee there will be zero downtime of the asset you are subscribing to.

We’re also moving towards a more interconnected economy, where many companies come together in partnership, bringing with them their own piece of expertise. The ecosystem that this creates depends on trusting others to do the right thing so that the whole thing works and delivers for everyone.

A data-centric world needs digital trust

We can only benefit from today’s data-centric world with transparency and trust. Trust and security in digital business models and the customer experience is no longer a nice-to-have; it’s an imperative.

Recently, we launched our Zero Trust Security Service, a highly secure environment designed to counter increasingly sophisticated cyberattacks amid changes in working styles, and greater use of cloud services and remote work environments.

This new offering is based on the introduction of a zero trust architecture to NTT Group’s 140,000 employees in 55 markets worldwide, as part of a global security governance overhaul. We’ve now systematized our expertise to provide customers with a comprehensive service, from consulting to architecture implementation and operation. Together with strategic global partners, NTT DATA has created a structure with more than 1,000 specialists able to provide services.

As such a central element to trust, security holds one of the keys to strengthening the relationship between businesses and our wider community. With data and information being so valuable and vast a resource to modern organizations, a zero trust approach to security is not only necessary but

“

Being transparent means having the humility to accept you have made mistakes. To own up, and to be straightforward about how you will avoid the same mistake next time, is the most powerful thing you can do.

lucrative: according to Forbes, global revenue for the zero trust market is expected to reach \$69.85 billion by 2028. Demonstrating trustworthiness pays dividends.

Trust equals value

Forward-thinking leaders understand that trust is an economic asset, and a crucial one. But more than that, placing trust as the new business imperative allows us, as organizations, to play a vital role in meeting global challenges head on.

Across society, we are facing challenges that we can only address together. The World Economic Forum recently wrote: “Purposeful, trustworthy businesses will play a key role in delivering ambitious programs for decarbonization, creating meaningful and fulfilling work, developing new technologies that solve entrenched problems, improving health and well-being, and achieving inclusive growth.” For me, this underlines that the purpose of business is to build trust – with stakeholders, employees and customers – and through that, deliver authentic services that meet genuine needs and legitimately improve lives.

Every organization is on the journey to be better at building trust. Being consistent is difficult, and being transparent means having the humility to accept you have made mistakes. To own up, and to be straightforward about how you will avoid the same mistake next time, is the most powerful thing you can do to prove you can be trusted. At NTT DATA we are on this journey too. As we strive to build trust not just through reliable services for clients, but through a diverse and inclusive culture,

we recognize that this is an ongoing imperative.

In their 2021 report on trust, Forrester called out that – by connecting with customers, attracting the top talent, and creating unrivaled models of engagement – trusted organizations will be those who succeed in the coming decade: “This is your moment to earn trust from your customers, partners and employees if you want to drive revenue-generating loyalty.”

I believe this is our moment, to prove that we are leaders that can be trusted; trusted to be drivers of meaningful change and cooperative action that, together, protects our future.

For references, please go to cxomag.com/article/trust-the-new-currency-of-business/



After joining NTT DATA in 2000, **Fernando Apezteguia** established a strong reputation for consultancy in the financial sector, working on numerous strategic banking projects for the Santander Group in Spain, Germany, Chile, Brazil and the UK. He went on to become Global Head of Banking for NTT DATA, overseeing the banking practice across Europe, Latin America and the US, before becoming CEO of NTT DATA in Brazil. He joined NTT DATA UK&I in 2021 and has been heading the organization as CEO since April 2022.

Why Trust is Stuck in the U-Bend

By John Elkington, Founder & Chief Pollinator at Volans, professor, and author of *Green Swans: The Coming Boom in Regenerative Capitalism*

We are facing a continuing erosion of trust in the institutions of capitalism, globalization and democracy. But with a focus on regeneration, instead of just responsibility and resilience, businesses can plot a course through this period of disruption and systemic change.

Brand value. Intangible assets. Social capital. The range of terms used to sell trust expands constantly. But so, too, does the casebook of calamities. The Dutch coined the proverb “trust arrives on foot, but leaves on horseback”, but there is no national monopoly on blunders denting our faith in people, brands or institutions. Think of Boeing in America, Vale in Brazil, Carillion and P&O in Britain, vaccination in China, or VW in Germany. Trust can now depart like a Tesla.

This matters because, as Edelman explains in the 2022 version of their Trust Barometer, trust is “the ultimate currency in the relationship that all institutions – companies and brands, governments, NGOs and media – build with their stakeholders. Trust defines an organization’s license to operate, lead and succeed. Trust is the foundation that allows an organization to take responsible risk, and, if it makes mistakes, to rebound from them.”

We used similar arguments at SustainAbility in the 1990s in launching our ‘Engaging Stakeholders’ platform, alongside the UN. Our aim is to help evolve greater levels of societal trust in business,

lubricating the sustainability transition. Systemic change, we concluded, would be quicker, cheaper and more effective with higher levels of trust.

Sustainability reporting surged, but the net result has been disappointing. Everywhere, trust is in retreat. As Edelman notes, “We find a world ensnared in a vicious cycle of distrust, fueled by a growing lack of faith in media and government.”

The continuing erosion of trust in institutions

Will we turn a corner soon? No, though new dynamics are evolving. Rachel Botsman spotlights three steps in trust-building: the ‘California Roll’ principle (make the novel seem familiar), tackling the ‘what’s in it for me’ barrier, and mobilizing ‘trust influencers’.

These are all sensible, but the evidence suggests that trust levels will decline well into the 2030s. There will be exceptions, with individual leaders, countries, organizations and initiatives shrugging off wider declines. And there are teachable lessons on how to manage and grow trust. But, overall, expect

a continuing erosion of trust in the institutions of capitalism, globalization and democracy. Why?

I explore the drivers in my latest book, *Green Swans*. Early on, I sketch where the future seems to be taking us. Bluntly, we are stumbling into a global ‘U-Bend,’ where – once again – an old order comes apart, while new ones struggle to find their feet.

Geopolitical and macroeconomic realities taken for granted since WW2 are disintegrating. China and Russia are turning their backs on what they see as a waning world order. Until we fix our global plumbing, trust levels will not regain their former highs, stuck in the U-Bend. Expect growing confusion, fear and anger.

Current responses to disruption aren’t fit for purpose

Businesses, industries, economies and even civilizations collapse. It is the natural order, and part and parcel of capitalism. The drivers include testosterone (think Putin), greed (recall the 2007-2009 contained depression) and myopia (the list is endless).



“

We are stumbling into a global ‘U-Bend,’ where – once again – an old order comes apart, while new ones struggle to find their feet.

Deeper currents are at work, too. Recall Joseph Schumpeter’s ‘gales of creative destruction.’ These implode old economic orders, radically shifting patterns of trust as elites lose their grip. Creative destruction is now simultaneously disrupting capitalism, democracy and globalization, so future declines in trust are pretty much baked in.

Most current responses are unfit for purpose. Think of the current feeding frenzy around environmental, social and governance (ESG) investing. This underscores just how weak a grip most financial people have on the forces now in play. They may swap their decks of cards, but play the same old game aboard the economic equivalent of the White Star Line’s ill-fated liner in 1912.

Most passengers on the Titanic trusted claims that the liner was unsinkable, just as we trust claims that today’s capitalism is sustainable.

Meanwhile, we continue to trust modern corporations even as they mislead, intentionally or not. Remember Carillion, the British supply chain company? I remember reading their latest ‘sustainability’ report, launched days before they collapsed into bankruptcy.

“Businesses without visionary engagement, inspiring stories, responsible compliance or public trust,” their Chief Sustainability Officer intoned,

“are businesses without competitive futures. For Carillion, sustainability is how we shape our competitive future, how we add value and how our people create even more inspiring stories for a better tomorrow.”

That text vanished from their website as bankruptcy loomed.

The regenerative economy

Clearly, our trust in business must be relative, informed and, crucially, critical. Healthy governance systems – the anchoring element in ESG – can moderate the excesses of capitalism, but not remove them.

“Trust but verify” was the Russian proverb adopted in nuclear disarmament negotiations. It should now shape all our interactions with business and financial markets. And the verification component will be make-or-break.

We must also challenge our own thinking. Back in 2018 I launched the first-ever product recall for a management concept, via the Harvard Business Review. My focus was on the Triple Bottom Line, which I had introduced in 1994. Ultimately, I concluded, “we have a hard-wired cultural problem in business, finance and markets. Whereas CEOs, CFOs, and other corporate leaders move heaven and

“

The change agenda for business is expanding from responsibility, through resilience to regeneration.

earth to ensure that they hit their profit targets, the same is very rarely true of their people and planet targets. Clearly, the Triple Bottom Line has failed to bury the single bottom line paradigm.”

The change agenda for business is expanding from responsibility, through resilience to regeneration.

But paradigms are shifting – and the change agenda for business is expanding from responsibility (‘corporate social responsibility’), through resilience (recall how supply chains are being disrupted by the pandemic and war) to regeneration. On the third of these, giant companies like Walmart, Pepsico and Unilever are now talking up their commitment to the ‘Regenerative Economy.’

Again, trust, engage – and verify.

Only when such actors commit heart and soul to systemic transformations will there be any chance of building deep, lasting reservoirs of trust. The challenge will be toughest for those surfing tomorrow’s tsunamis – and if you want clues as to the scale of those impending disruptions, track down RethinkX.

Paradoxically, though, trust-building may ultimately be easier for successful disruptors.

Do you trust Elon Musk? It hardly matters. His success in disrupting one sector after another links him with progress people want to see. And we tend

to invest our hope – and eventually trust – in those we see responding to our biggest challenges. As they stretch into the future, we come to feel part of their team. Intangible, but invaluable.

For references, please go to cxomag.com/article/why-trust-is-stuck-in-the-u-bend/



John Elkington is one of the founders of the global sustainability movement, an experienced advisor to business, and a highly regarded thought leader and keynote speaker. In 2008, The Evening Standard named John among the ‘1000 Most Influential People’ in London,

describing him as “a true green business guru”, and as “an evangelist for corporate social and environmental responsibility long before it was fashionable”. In 2009, a CSR International survey of the Top 100 CSR leaders placed John fourth: after Al Gore, Barack Obama and the late Anita Roddick of the Body Shop, and alongside Muhammad Yunus of the Grameen Bank.

How Companies Can Build Trust in Uncertain Times

By Shalene Gupta, Research Associate at Harvard Business School and co-author of *The Power of Trust*

Trust can take years for organizations to build with customers and employees, but only moments to break. How can businesses secure and build trust that can stand the test of time in a turbulent period of economic shakiness, political unrest and a global pandemic?

“

Trust has a real and tangible impact on a business's bottom line.

Companies are always being judged on whether they warrant our trust: as customers, employees, investors or members of the public. Right now, every company is either building trust through their actions, losing trust or recovering trust they've lost. In this time of uncertainty – a global pandemic, war, supply chain challenges – trust is more important than ever before. But what is it and how do organizations go about building it?

Trust is our willingness to be vulnerable to the actions of others because we believe in their good intentions toward us. This isn't just a nice-to-have. It has a real and tangible impact on a business's bottom line. In a study of 30 NCAA basketball teams, those that trusted their coaches won 7% more of their games than teams that didn't. In addition, the team with the highest trust in its coach had the highest number of wins. This translates to revenue gains. In another study of Holiday Inns, an 1/8 point increase in trust in managers (on a scale of 1-5), correlated to a 2.5% – or \$250,000 – increase in revenue. Scale this up, and we see a huge impact on economies. In a World Bank study of 29 market economies, a 10% rise in trust in the population correlated with 0.8% increase in GDP.

Competence and motives to develop trust

There are four key elements that build trust: competence, motives, fairness and impact. The foundation of trust is competence, a company's ability to build products and services that work well and live up to their promise.

According to a study by University of Singapore professor Daniel McAllister, people must trust in each other's competence before they can trust in other more emotional aspects of trust. Consider Uber, the ultra-popular rideshare app. Uber transformed the taxi industry simply by making it easy to find, book and pay for a cab. In 2015, five years after Uber launched, it had 11 million users; the year after it grew to 37 million users, and by 2017 Uber's users had skyrocketed to 68 million.

However, competence alone is not enough. In 2017, a slew of Uber scandals made headlines ranging from sexual harassment to shady business practices. Ultimately, CEO Travis Kalanick had to leave. During the same period, Uber's competitor, Lyft, who provides the exact same service, saw its market share grow twice as fast.

Stakeholders also care about a company's motives: that is, they want to know whose interests a

“

The final element of trust is impact. You can nail competence, motives and fairness, but if the overall impact on other people is still negative, that's what they'll remember.

company serves. We all understand that companies need to make a profit. However, as customers we expect that when we buy a product or a service, it will live up to its promise. Then, as employees we expect the company will not actively try to harm us and take a reasonable amount of care to ensure our wellbeing. As investors, we expect transparent and accurate disclosures so we know what to do with our money, as well as wise decision-making from company leaders so we know our investments aren't being squandered.

This may seem obvious, but remember CEO Elizabeth Holmes of Theranos was able to get more than \$700 million in investments, when her product – claiming to revolutionize blood testing – was simple fraudulent science. We cannot actively police everything a company does: in order to engage with a company, whether it's as a customer, employee or otherwise, we have to generally trust that they have good motives and do not intend to hurt us.

Fairness and impact in trust building

Good intentions also need to be translated into action, which leads us to the next element of trust: fairness. There are four different types of fairness. The first is procedural fairness, which means the

company has good processes, based on accurate data, that are used to make decisions and are applied consistently, and whether groups are given a voice in decisions affecting them. For example, at the Ritz-Carlton, managers invite, indeed expect, employees to offer feedback on processes.

Next is distributive fairness which is how resources such as pay and promotions or pain points such as layoffs are allocated. Employees at the Ritz-Carlton, including servers and housekeeping, are offered competitive pay as well as full medical, vision, dental and retirement match benefits. Then there's interpersonal fairness, which is how well stakeholders are treated. The Ritz-Carlton treats even the employees they don't hire to a respectful interviewing experience, a box of miniature Ritz-Carlton chocolates, and a fond farewell when they leave. Finally, there's informational fairness, which is whether communication is honest and clear, and if the people who are impacted by a decision receive the relevant information about it in a timely manner.

The final element of trust is impact: the effect a company's actions have on other people's lives. You can nail competence, motives and fairness, but if the overall impact on other people is still negative, that's

“

We live in an ever-changing world. Companies cannot offer any guarantees about the future: however, what they can offer is the promise that they will continue to do the best job they can.

what they'll remember.

For example, in 1958 Chairman Mao decided that he wanted to reduce disease and improve crop yields. He dreamt up the Four Pests campaign, where peasants were rewarded for turning in the bodies of pests – including sparrows, which ate roughly 10 pounds of grain a year. People who handed in sparrow carcasses received a reward. Overall, the campaign was a success: people killed a total of one billion sparrows. The campaign was competent, the motives of increasing crop yields were positive overall, and the campaign was fair – people got their rewards.

However, it turns out that sparrows eat locusts. Without sparrows to keep the locusts under control, the locust population ballooned. Locusts swarmed the land, gobbling up crops. This triggered the Great Chinese Famine, which killed over 30 million people. Today no-one is talking about the brilliant trust success of the Four Pests campaign, even though the impact was unintentional. Whatever the impact is – even if it's unintended – to remain trusted, you have to take responsibility for it.

Trustworthy intentions

The Nobel Prize winning economist Kenneth Arrow once stated that nearly every economic transaction has an element of trust. We live in an ever-changing world where it's impossible to figure out what will happen next. Companies cannot offer any guarantees about the future: however, what they can offer is the promise that they will continue to do the best job they can, work to help rather than harm people, be as fair as possible, and take full responsibility for the impact they create. In a word, they can work towards being trustworthy.

For references, please go to cxomag.com/article/how-companies-can-build-trust-in-uncertain-times/



Shalene Gupta is the co-author of *The Power of Trust* with Harvard Business School Professor, Sandra Sucher. She has previously been a Research Associate at Harvard Business School, a Reporter at Fortune and a Fulbright Scholar. She is currently working on her second book.

5 Minutes On...

Trust as the Driving Force of Business

By Shalene Gupta

Research Associate at Harvard Business School and co-author of *The Power of Trust*



5 Minutes On... why trust is not a complex idea, but it does have elements that should be played out correctly by businesses for it to be effective. Where many businesses fail is understanding how to recover trust and how to maintain it in the long term.

Scan the QR code with your smartphone camera



Empathy and Trust: The Human Engine in Organizational Performance

By Alex Allwood, CX expert and author of *Customer Empathy: A Radical Intervention in Customer Experience Management and Design*

On the back of the biggest ever global economic shutdown, organizations embraced empathy and trust as the newest workplace traits. As we begin to experience some semblance of normalcy, there is a window of opportunity to leverage this rediscovered state of 'humanized connection' for customer-led empathy to improve people and business performance.

Collectively, during the pandemic, we deepened our connection and humanized our working relationships. We leaned into being vulnerable, sharing our stories, listening and perspective-taking, experiencing together and acting with compassion. Leaders supported their teams to get them operational, adapt to working virtually and manage their wellbeing. This delivered a new state of shared empathy, deeper connections and a new culture of organizational trust.

Paul Zak is the Founding Director of the Center for Neuroeconomics Studies, Professor of Economics, Psychology and Management at Claremont Graduate University, and author of *The Trust Factor: The Science of Creating High Performing Companies*. Over two decades his research has shown a direct correlation between oxytocin (a hormone that helps nerve cells in the brain send messages) and empathy. Zak's research found oxytocin is essential for creating trustworthy relationships. Simply put, increased oxytocin increases empathy and increased empathy equals deeper human connection.

Conclusively, his research has found a clear relationship between organizational trust and business performance, where "Compared with people at low-trust companies, people at high-trust

“
Simply put, increased oxytocin increases empathy and increased empathy equals deeper human connection.”

companies report 74% less stress, 106% more energy at work, 50% higher productivity, 13% fewer sick days, 76% more engagement, 29% more satisfaction with their lives, and 40% less burnout.”

Customer empathy as a powerful resource

Just as employee empathy empowered shared understanding of experiences during the pandemic, so can customer empathy be switched on to help employees understand and feel what it is like to be a customer. For the most part, customer empathy is underutilized in business and mainly utilized in human-centered design. When scaled across the business however, customer empathy is a powerful human resource to unlock divergent thinking by bringing fresh points of view into day-to-day customer problem-solving and decision-making.

Currently, there is a conventional belief that employee empathy equals customer empathy. However, employee empathy alone is not sufficient to develop deeper and more meaningful customer connections; especially for non-customer facing employee teams. To enable employees to take the perspective of the customer requires bridging the 'empathy gap'. This gap is perpetuated through:

- A shortfall in empathetic leadership, such as the very poor treatment of customers brought to light in Australia recently by Royal Commissions into Banking, Insurance and Aged Care;
- The siloed mentality within organizations, where businesses are still organized by business units or functional groups to reduce complexity and increase productivity and efficiency. The upshot is employee teams that don't work together in the best interests of customers;
- Then the obsession with representing customers as scores, statistics and graphics. This reduces the visibility of customers as human beings, diminishing employees' ability to develop a shared customer connection – and effectively shrinking the customer's perspective to just another number on their PC dashboard.

Empathy-led innovation and customer feedback

Cleveland Clinic is an excellent case study of empathy-led innovation in culture and organizational structure as a driver of customer satisfaction and business performance. Cleveland

“

There is a conventional belief that employee empathy equals customer empathy. However, to enable employees to take the perspective of the customer requires bridging the ‘empathy gap’.

Clinic is one of the largest medical center groups in the US, with 10 hospitals and 19 medical centers, 40,000+ staff and an operating budget of \$6 billion. Their innovation started with a critical piece of customer feedback: “We know about Cleveland Clinic and the excellent results you deliver. But we decided not to go there because we have heard you have no empathy. We went to another hospital instead, even though it wasn’t as highly ranked.”

At the time, Dr Delos ‘Toby’ Cosgrove, esteemed heart surgeon and Cleveland CEO, pondered: what if medicine was defined from the patient’s perspective, what if patient care was designed from patient experience, and what would this mean for how hospitals were organized and medical services delivered?

Through active listening to patient/doctor conversations, he reimagined the distinction between surgeons and physicians, arguing that patients did not ask for particular specialists but instead described their symptoms and how these made them feel. “When people were sick they did not say, ‘I need a cardiothoracic surgeon’ or ‘Take me to a cardiologist’. Instead, they would declare ‘My chest hurts’ or ‘I can’t breathe’ – or simply ‘I feel unwell.’”

Ultimately, the business decided not just to

reorganize, but to redesign medicine to deliver a customer experience that felt human – breaking down the specialist silos and challenging long-held medical conventions.

In 2008, before their customer empathy-led transformation, Cleveland Clinic ranked last in patient satisfaction. Five years later, they ranked number one.

A culture to make you feel good

Embedding a culture of customer empathy requires building a solid foundation of trust, signaling to employees that empathy isn’t just the next corporate buzzword. The challenge for organizational leaders is working within the constraints of their corporate system – the business’s current ways of working and shifting biased mindsets. To foster engagement, employees need to see less talk and more action. The first step is humanizing how leaders think, act and communicate.

To create a culture of trust that will raise oxytocin levels, elevate empathy among employees and enhance organizational performance, Zak prescribes, amongst other strategies, showing vulnerability. Zak argues in a Harvard Business

“

Reviewing a business’s performance metrics is critical to ensure congruence with the organization’s cultural aspirations, and aligning these business goals with recognition and reward.

Research Journal, *The Neuroscience of Trust*, “Leaders in high-trust workplaces ask for help from colleagues instead of just telling them to do things. My research team has found that this stimulates oxytocin production in others, increasing their trust and cooperation. Asking for help is a sign of a secure leader – one who engages everyone to reach goals.” It’s like the pre-flight announcement before flying: make sure you put your oxygen mask on first before helping others.

A robust customer empathy program includes developing and scaling customer listening with empathy and customer storytelling. Also necessary is utilizing tools such as customer journey maps with emotion graphs, formalized service safari programs and the like, that facilitate ongoing customer conversations and humanize the customer’s experience, especially for back-of-house and cross-functional teams. Empathy nudges too, such as skills and practices that can provoke empathy, are a proven method for delivering behavior change. The process of reviewing a business’s performance metrics is critical to ensure congruence with the organization’s cultural aspirations, and aligning these business goals with recognition and reward.

Overnight (and by necessity), humanizing the workplace with empathy and trust became the new black. Now, with growth back on the agenda, the imperative for organizational leaders is to leverage this rediscovered state of ‘humanized connection’ for customer-led empathy to enhance their people and business performance.

For references, please go to cxomag.com/article/empathy-and-trust-the-human-engine-in-organizational-performance/



Alex Allwood is a customer experience strategist with expertise in qualitative research and consumer behavior. A recognized customer-centric practitioner, Alex’s method connects ‘customer and culture’ to put customer needs at the center of leadership, strategy and operations. Alex has authored two books, the latest being *Customer Empathy: A radical intervention in customer experience management and design*.

The Human Side of Risk

By Edmund Tribue, VP Risk & Compliance, & Kim Curley, VP Workforce Readiness Consulting, NTT DATA Services

In such turbulent times, with a global pandemic and the drive towards the digital world, dependence on cyber safety and consumer trust only becomes increasingly important. Technology continues to develop in complexity, as do our methods to mediate it, but it's imperative that we don't forget the human side of risk, too.

In July 2020, cybercriminals orchestrated one of the most high-profile hacks of the year. At the start of the pandemic, employees worldwide shifted to remote work models, including staff at Twitter. It was then that cybercriminals impersonated Twitter IT Administrators and persuaded top employees to disclose account credentials. This series of events led to an elaborate crypto scam, including the fraudulent takeover of 130 high-profile accounts, including Barack Obama, Joe Biden and Kanye West. Twitter later released a statement announcing that its own employee tools contributed to the unprecedented hack. The entire ordeal led to a 4% decrease in Twitter's share price and extensive reputational damage. The criminals didn't leverage sophisticated technologies, malware or exploits to pull off this hack. Instead, they used social engineering tactics to infiltrate a \$37 billion technology company.

We humans are complex, unpredictable, and at times, risky. The Twitter scam demonstrates that although the waves of the pandemic, remote work and highly skilled cybercriminals contribute to

increased enterprise risk, one of the most challenging factors to manage is the human side of risk.

To prepare for the next frontier of risk management, leaders must start with a human-centric approach to risk modeling that addresses the intersection of people and risk at scale. Commitment to risk management is a commitment to earning the trust of your teams, developing a corporate culture of risk awareness, and eventually, strengthening the trust and loyalty to your consumers.

The human impact on risk management and compliance

Enterprise risk management (ERM) refers to the methods and processes that organizations use to mitigate risk, including identifying threats, assessing the magnitude of impact, crafting a response strategy, and continuous monitoring. Protecting an enterprise must include three critical areas: governance, risk management and compliance (GRC).

- **Governance:** Ensuring that all organizational activities are aligned to support overall goals,

(IT operations, training, human resources).

- **Risk Management:** Identifying, assessing, and controlling threats to the business (cybersecurity, legal consequences, natural disasters).
- **Compliance:** Aligning internal organizational activities with external laws and regulations (legal mandates, environmental laws, privacy).

Addressing the human side of risk is one of the most effective yet undervalued GRC strategies. Employees are especially prone to impacting risk management. All too often employees click links in phishing emails, end up being manipulated to provide access and information during social engineering attacks, use weak passwords, accidentally download malicious hardware, or make errors that cause security incidents. Incredibly, 88% of security breaches result from human error, and 37% of attacks involve emails as the root cause of breaches.

Humans not only impact security protection and risk management, but also influence compliance efforts. For example, imagine an IT department



“

Commitment to risk management is a commitment to earning the trust of your teams – and loyalty to your consumers.

employee identifies an outdated software containing gaps that could lead to a breach. In a risk-aware culture, this employee would be celebrated for reporting and remedying this issue. However, in a risk-avoiding culture, this same employee may not understand the significance or choose to overlook the gap due to a lack of clarity around risk management processes. Overall, whether it's security protection, compliance, or general risk awareness, your organizational governance and risk culture will inform how well your people can protect your business.

Overcoming obstacles and embracing best practices

First, organizations need a clearly-defined risk strategy. Without direction, it's easy to continue with business-as-usual; but the ultimate goal must be to establish governance and a culture of risk awareness, where key decision-makers define objectives and employees participate in continuous training and consider risk in everything they do.

Many organizations allow pressure for operational cost reductions to limit spending on risk programs, particularly effective training. Leaders at the top may not demonstrate risk awareness or advocate for the importance of risk management.

Often, employees who put organizations at risk are doing so simply by mirroring the corporate approach to risk management. Fortunately, there are practical ways organizations can inspire employees to care about risk management and compliance. It starts with leadership.

Leaders need to encourage teams to take threats seriously and abide by best practices. While investment in IT infrastructure, controls and programs driven by a Chief Information Security Officer (CISO) should continue, the human factor remains a considerable risk. Organizations want to trust their teams to mitigate risk, but first, leaders must provide necessary support. We see three actions that organizations can immediately prioritize to make an impact on GRC.

1. Align leaders and create visibility from the top

Starting at the top, Chief People Officers and Chief Learning Officers must form a tighter and more formal link with Chief Risk Officers and CISOs to create alignment for human-centric strategies that integrate the company's enterprise risk profile into culture, awareness and training.

Leaders educated on specific risks must act as an accountable voice, promoting and communicating the importance of risk management and compliance.

“

Your organizational governance and risk culture will inform how well your people can protect your business.

Companies must ensure that leadership is the face and voice of risk management, as they lead by example in meetings and everyday behaviors.

2. Build a culture that will drive behavior and action to maintain security across the organization

Culture drives beliefs and actions beyond what the best controls can accomplish. Culture, as it relates to driving behavior, can be an additional line of defense in managing overall risk. Therefore, leaders who wish to foster a risk-aware culture must make the effort to create lasting adoption of the right behaviors.

The first step in creating sustainable culture change is awareness and education. Organizational risk awareness campaigns bring increased visibility to security threats and the associated risks through videos, newsletters, articles and other mediums. Next, leaders must identify and implement policies and procedures that support the right actions, celebrating the risk-aware behaviors, and providing reinforcement for those that run counter to the strategies. Finally, organizations must align performance management processes to the desired outcomes, tailoring them to roles, including data protection and prevention.

3. Deploy formalized, immersive training to build mastery of common threats

Employee awareness and behavior rely on the quality and relevance of organizational communication and training programs. Therefore, organizations must move away from dry, annual slide deck presentations to engaging and realistic training that prepares teams for the modern risk landscape.

To support retention of the training, companies can scale gamification techniques, such as leaderboards, to reinforce desired behaviors and increase participation. Training programs can and should be more engaging and relevant (for example, scenario-based simulations bring awareness to different security threats and how to best respond), and as not all employees have the same risk profile, training should be tailored across different roles and teams.

Personalized risk training deepens lessons and resources in protecting data. In these training sessions, employees may realize the importance of security protection in their lives outside of work, and bring this mindset with them as they enter the workplace. This relatable content can drive engagement as employees learn to make their personal data more secure.

“

Change requires communication, education, behavioral strategies and trust. As a leader, if you want to trust your people to protect your organization, start by proving that they can rely on you.

Creating a future-fit, risk-aware culture

The next frontier of risk is all about humans in the workforce. Organizations will recognize the importance of reskilling and upskilling their people to understand and avoid common threats. Global spending on IT and risk management will continue to grow; in 2020, spending grew 6.4% and in 2021, it doubled its growth to 12.4%. Global spending on security awareness and phishing simulation programs alone are predicted to reach \$10 billion by 2027.

The future of work and risk will also see increased regulatory oversight. Organizations will embrace incentives and consequences associated with compliance efforts, and feel added pressures to build a robust risk management strategy. Even the external public, including clients, stakeholders, and consumers, will feel a heightened awareness of potential risks and strategies to protect their data and reputations.

In the end, sustainable change depends on culture. It's not enough for organizations to bolster risk management spending or introduce a cutting-edge technology solution and expect people to change accordingly. Change requires communication, education, behavioral strategies and trust. As a leader, if you want to trust your people to protect your organization, start by proving that they can rely on you. Grant your teams the knowledge and tools needed to successfully manage existing and emerging risks.

For references, please go to cxomag.com/article/how-the-circular-economy-benefits-business-and-investors-while-tackling-global-challenges/



Edmund Tribue is the Risk and Compliance Practice Leader for NTT DATA Services. With more than 30 years of experience in the financial services industry, Edmund has held senior positions focusing on consumer and small business lending and credit

management functions, acquiring vast experience in Lifecycle Credit Risk Management, Operational Risk Management, Fraud Management and Regulatory Compliance. Prior to joining NTT DATA, Edmund was Director for Card and Payments at PwC. A member of many industry groups, Edmund publishes regularly in trade publications on risk, AML and KYC.



Kim Curley has spent her career focused on the human side of business, enabling leaders and their organizations to do more, do better, and to thrive through change. As the Workforce Readiness Consulting Practice Leader for NTT DATA Services,

Kim leads advisory consultants who deliver people-side consulting solutions that help our clients solve their most complex business challenges.

In Depth

NTT DATA takes a deeper look into critical areas of business trust.



Building Trust in Artificial Intelligence

Big data and fast computing power has moved artificial intelligence out of the laboratory and into the workplace, with the predictions that AI systems make becoming, in many cases, a must-have to drive change and growth. But our inability to understand and interrogate the decisions being made – because of the lack of explanation as to how it works – reduces confidence and our ability to fully trust the AI system. What can help us uncover the AI engine’s inner workings?

Scan the QR code with your smartphone camera



Building Trust in Artificial Intelligence
 Explainable AI is the way forward for making systems transparent and dependable

APRIL 2021

© 2021 NTT DATA, Inc. All rights reserved. NTT DATA

Ushering in a New Era of Customer Engagement with Digital Twins

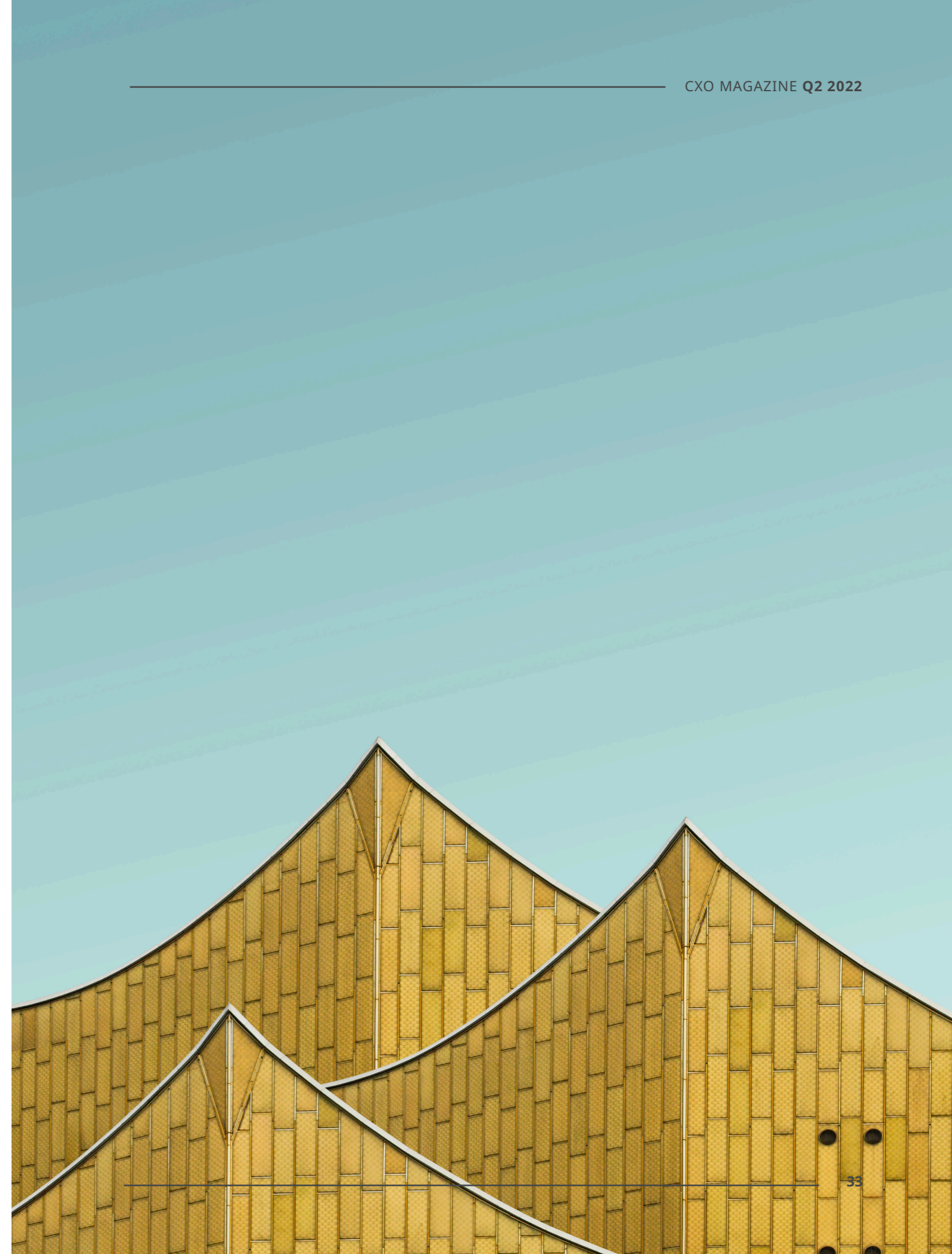
By David de Castro Pérez, Innovation Manager, NTT DATA Europe & LATAM

It's the next big thing in understanding and engaging customers: building a virtual replica of the business ecosystem, and leveraging ontologies as enabling technology. This exciting branch of AI can help businesses to generate very targeted insights into their customers' expectations and needs.

Customers are, by definition, placed at the core activities of every business. And regardless of its nature, size or sector, every business struggles to better understand, approach and engage its customers. The better businesses understand their customers – their expectations and needs – the more they can nurture lasting relationships with them, relationships built on mutual trust.

From the company's point of view, these relationships are fostered with a very clear goal: commercial success. But customers have clear expectations of the relationship too. In the hyper-connected world we inhabit today, customers expect companies not only to meet their needs, but to understand, anticipate and often exceed them. To achieve that, businesses must build data-driven, customer-centric strategies to both gain and maintain a solid customer base.

Of course, customer data is essential both to optimize the customer journey and to drive customer engagement. However, dealing with this data is often a very time-consuming and inefficient task, which prevents companies from creating the



“

Data flows from the physical product to the digital twin, and information from the digital twin flows back to the physical environment. This concept has the potential to become the cornerstone for the creation of a virtual replica of individuals or a business ecosystem.

hyper-personalized, memorable experiences that clients demand. This situation can be improved by applying, in a revolutionary way, the concept of digital twinning – i.e. using real-world data to create simulations to make predictions and aid decision-making – in the customer data management domain.

From data to knowledge

Digital twins have ranked steadily as one of the most promising technologies for the past 10 years, with Accenture rating them as one of the top five technology trends in 2021. Digital twins originated in the industrial sector, where virtual replicas of physical systems (say, a factory or an engine) were created. This concept consists of three different parts: the physical product, the digital/virtual product, and the connection between the two products.

The connection between the physical product and its digital twin is data – data that flows from the physical product to the digital twin, and information from the digital twin that flows back to the physical environment. This concept has the potential to become the cornerstone for the creation of a virtual replica of individuals or a business ecosystem. However, it should be clear when contemplating this idea that a person is far more complex than any

physical system (no matter the number of sensors or states that are needed to describe it). Therefore, an additional technology lever needs to be incorporated into this approach, namely ontologies.

The word ontology refers to ‘the nature of being’ as well as ‘a set of concepts (in a particular domain) and the relations between them’. With regard to digital twins, an ontology is a systematic, extendable model. It consists of entities, their attributes, and relationships among them. These can be used very efficiently for the representation of a knowledge domain. It is also very suitable for integrating data in a meaningful way, data that could potentially come from any source.

We can visualize this as a three-layered architecture, with the first layer (generic knowledge) enriched by two additional extensions:

- Generic customer knowledge domain (applicable to any business)
- The knowledge specific to a given industry or sector
- The client needs and business models of a given company.

In practical terms, this would mean going from generic information to much more specific information addressing business needs and specific use-cases from different business sectors.

“

Practical applications for a virtual replica of a company’s customers and business ecosystem are almost limitless... testing commercial hypotheses, defining market strategies, designing new products, or analyzing personalized marketing actions – all with no risk and at no cost.

From knowledge to practice

This combination – a digital twin approach plus ontologies – allows companies to shift from a situation where data itself is the concern, to a new one where profit-driven knowledge generation is the goal. In other words, this approach would enable the definition of strategies and, also, novel relationships with clients, based on the most advanced (and significantly richer) customer profiling and representation. Furthermore, it will allow organizations to generate valuable insights due to ground-breaking forecasting and simulation capabilities enabled by ontologies.

The potential practical applications for a virtual replica of a company’s customers and business ecosystem are almost limitless. For instance, we can foresee testing commercial hypotheses, defining market strategies, designing new products, or analyzing personalized marketing actions – all with no risk and at no cost.

This approach adopts the perspective of companies, i.e. of marketing executives or strategists in big organizations. Now, what would happen if we took a Copernican twist, changing the perspective from corporations to people – and let customers gain control over their digital twins?

What if we empowered them to express their

consuming preferences, to nurture their virtual replica over time, to connect through their avatar with all kinds of companies in a centralized way, and to interact with other customers’ avatars?

From practice to trust

Heady as the possibilities are, we must never lose focus on keeping customers safe – both in physical and digital environments. Only through responsible, safe practices can trust be maintained between businesses and customers.

As with every system dealing with personal data, security is a crucial consideration in digital twin technology. Moreover, bias in artificial intelligence based systems is a known challenge: because AI systems are typically based on machine learning algorithms – and made by humans – prejudiced assumptions can be made during the algorithm development and, more importantly, these systems need training, so prejudices can enter into that process too.

For instance, in 2014, software engineers at Amazon built programs that review resumés of job applicants – and realized later that the system discriminated against women for technical roles. In 2019, San Francisco legislators voted against the use of facial recognition, because they believed

“
The bigger picture is that the combination of digital twins and ontologies allows us to envision revolutionary spaces where individuals can express themselves and engage in fulfilling experiences.

they were prone to errors when used on women or people with darker skin tones.

Therefore, this solution has to be compliant by design – meaning that every legal and ethical concern or risk must be taken into consideration from the earliest conceptualization stages, and throughout product development. This will ensure that these principles are observed, embedded and interwoven into the very fabric of the product. Furthermore, legal experts need to be involved to deal with data protection issues and intellectual property matters. Those details can be ironed out, however. The bigger picture is that the combination of digital twins and ontologies allows us to envision revolutionary spaces where individuals can express themselves and engage in fulfilling experiences. A customer digital twin is an initial (and necessary) step towards the foundation of such new worlds.



David de Castro is a Manager in the Innovation and Strategic Investments unit in NTT DATA EMEAL where he leads transformational initiatives. Based in Madrid, as an engineer with an MBA, he has a long track record in innovation management, business development and strategic consultancy. Before, he led research and innovation activity, as Head of Innovation, in a group of companies which operates in the aerospace and security sectors.

For references, please go to cxomag.com/article/ushering-in-a-new-era-of-customer-engagement-with-digital-twins/

The CXO Podcast

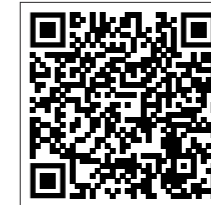
Available now on Apple Podcasts and Spotify

Or scan the QR codes to listen on CXOmag.com

The CXO Podcast: Purpose Strategy Meets Talent Strategy

In this episode of the CXO Podcast, host Joe Trainor talks to CEO of brand purpose agency Given, Becky Willan, and NTT DATA’s managing director of Future of Work, Ric Garner, about how to make your business a force for good, how to build trust in a digital world, what employees today are really looking for, the dangers of purpose-washing, and how to get started in putting purpose at the heart of the business.

Scan the QR code with your smartphone camera



The CXO Podcast: Safeguarding Our Digital Lives

In this episode of the CXO Podcast, guest host Tom Winstanley talks to global cybersecurity expert and former police officer Jake Moore, and NTT DATA Business Solutions’ Head of AI & Robotics, Thomas Nørmark, about keeping ourselves safe online, from the threats posed by bad actors and cybercriminals to how we can establish and maintain trust when implementing new, disruptive technologies.

Scan the QR code with your smartphone camera



Protecting Data Starts With Good Governance

By Eva-Maria Scheiter, Head of GRC Consulting, NTT DATA DACH

Whatever the trigger, significant technological and other business changes should never damage your customers' trust in you. This means keeping their personal data safe. In fact, done well, data protection ought to increase confidence in your business. How to get there? It starts, as with many things, with a detailed understanding of the challenges and strong governance around the solutions.



“

If legal aspects of data protection have moved relatively slowly over the last 50 years, the same cannot be said for technology. How much data we share and how and why we share it have changed beyond measure.

If you are currently accountable or responsible for processing data, you might be feeling the pressure. Today, it feels customers are more demanding and cyber-crime threats are growing daily. However, it's worth pausing to reflect. Today, data protection, in general, is increasingly perceived as adding value.

This is backed by survey data. For example, the proportion of German consumers who were sure, or very sure, their data was safe on the internet grew from 13% in 2014 to 29% in 2020. In our cynical world, this improvement feels worthy of celebration.

As well as this steady improvement and development, our Governance, Risk and Compliance (GRC) teams are usually involved when our clients are planning or expecting major strategic changes that may directly or indirectly impact on data use.

All our work is based on capturing and responding to customer requirements. Each comes with unique data flow and storage arrangements, for example. They will come with their own project technical and commercial measures of success in place. Their attitudes to risk will also differ. A luxury retail client, for example, might put greater weight on protecting data than its competitors. Harrods of London is famously intolerant of tabloid snooping. Finally, each customer will apply data protection law according to their own interpretation.

Despite this varied and complicated picture, there

are enough commonalities across our work and established best practice to share key lessons.

A brief history of data protection

IBM's System/360 hardware arrived on the scene in 1964 as the first real commercial computing solution. Germany's first data protection legislation followed in 1970. In September that year, the Hessian State Parliament passed a Data Protection Act. The next big step in German data protection law came in 1983. The Constitutional Court established fundamental rights of informational self-determination. These state that individuals own, and can control, their personal data.

Other countries' legal frameworks generally followed in parallel. The current EU-wide General Data Protection Regulation (GDPR) came into force in 2018. It should be noted that it's best practice to assume the provisions of the GDPR apply to any organization processing data of EU citizens. We helped a client in Switzerland, for example, keep their German employees' data safe in line with EU law.

If legal aspects of data protection have moved relatively slowly over the last 50 years, the same cannot be said for technology. How much data we share and how and why we share it have changed beyond measure. The scale is immense. The world is expected to be juggling 175 trillion gigabytes (zettabytes) of data by 2025. One hundred trillion

“

Rather than acting as a barrier to change, keeping data safe and secure ought to be seen as a valuable addition to improvement.

seconds equates to three million years, if you were wondering how big that number was.

In the case of our personal data, this all needs protecting and, at the same time, to be instantly accessible. We are now used to using our smartphones to do everything, from paying bus fares and buying coffee to monitoring our health and watching the latest blockbusters. As a result, the technology surrounding data protection has become an incredibly complex landscape.

Why change data protection in your business?

If changing data protection policies and procedures in 2022 is difficult, why do it? A trigger for some is, naturally, a breach of the rules. Examples still regularly reach the press such as a Dutch airline, fined €400,000 for letting hackers download 83,000 customer records. Financial costs aside, the real impact of being caught is reputational. Problems, once identified, need to be taken seriously and improvements implemented transparently. Trust is easily lost and is hard to recover.

Change, however, needn't be a response to bad news. NTT DATA's work is often part of positive business planning. We helped a bank modernize, for example, as they moved away from fixed infrastructure to the cloud. The GRC Consulting team often works with clients around outsourcing

business processes too. Successful human resource management depends on efficient and secure management of employee data. Organizations wishing to manage customers through third parties also need to carefully consider where and how their data is shared.

In these circumstances, data protection can fall into the trap of defining what can't or shouldn't be done. This view is always an important one to challenge. Rather than acting as a barrier to change, keeping data safe and secure ought to be seen as a valuable addition to improvement.

In the effort to not fall into this trap, it can be challenging to know where to start. We recommend beginning by building a data governance framework that takes into account different data processing requirements in an integrative approach.

Start with good governance

It is important to leverage the capabilities of the entire enterprise as you consider the data protection organization within it. Working in silos is best avoided.

It is here where you define your data handling strategy, including setting protection goals and defining roles and responsibilities. You should take into account and supplement specifications and guidelines from various management systems too. Data protection, information security and risk management all need to be involved.

“

Outside eyes can galvanize efforts across different business units and project teams.

It pays to be pragmatic and balanced. Policies that are too restrictive can be just as damaging to your business as those seen as too lax. This will also depend on how mature your organization is. If it's well-established, a light touch may be all that's required. If you're still at the very beginning of your journey, you may need to prioritize data protection to avoid it becoming an issue down the line. It is often useful to get external help here. Outside eyes can galvanize efforts across different business units and project teams. An external Data Protection Officer might prove a catalyst.

Whatever your starting point, with a strong data governance framework in place, you're well on your way to keeping data safe in the long run. What's more, your customers, colleagues and the wider communities you work with will have greater confidence in you. Building and extending trust is always the goal.



Eva-Maria Scheiter manages complex, cross-company projects and programs for national and international clients in Governance, Risk & Compliance (GRC). Her focus of 20 years experience lies in the areas of information security, data protection, risk management, business continuity management and compliance.

For references, please go to cxomag.com/article/protecting-data-starts-with-good-governance/



VIDEO

Disruption, Trust and Value in the Fishing Industry

Ronald Aroca CEO, Tecopesca

Sustainable development requires a developed strategy, where a disruptive approach could reap far more benefits than sticking to traditional methods. Tecopesca has been taking bold steps to address the many challenges facing the industry today.

Scan the QR code with your smartphone camera



Nurturing Inclusivity and Productivity in a Hybrid World

By Pragma Limbu, Principal Consultant, Business Consulting, NTT DATA UK

Businesses must continue to navigate the evolving relationship between employers and employees to ensure a happier and productive workforce. Setting clear expectations and empathizing with individual motivations and priorities encourages transparency, and helps to build a trusting culture in the organization.

In 2019, just over 5% of people in the UK reported working from home regularly. With the onset of the Covid-19 pandemic, that figure rose to 46.6% in April 2020 as we witnessed an unprecedented shift in the working landscape. Although restrictions have now been lifted, new working patterns are here to stay, with 36% of working adults reporting working at home at the beginning of this year.

As we moved beyond the initial phase of the pandemic, we witnessed the dawn of a new kind of worker and a new model of working. Across industries and countries, hybrid working is now the norm. In fact, 63% of organizations surveyed by the CIPD in 2021 reported that they planned to introduce or expand hybrid working.

While working patterns have shifted, businesses are also having to navigate an increasingly acute shortage of talent. Almost half (45%) of employers have hard-to-fill vacancies, according to the CIPD. In response to this challenge, 48% are raising pay and 46% are advertising more jobs as flexible. Driven by ongoing skills shortages, organizations are being



“

Hybrid working has changed the nature of the psychological contract... expectations have changed, and a hybrid environment, while more flexible, calls for greater trust.

incentivized to develop working practices that are inclusive and productive for all.

A new psychological contract

Hybrid working hasn't just changed the individual lives of employers and employees, it has also changed the relationship dynamics between them. In any working environment, a psychological contract exists between the two parties – typically defined as a sense of fairness and trust. Psychological safety is one of the key indicators of a team's performance, enabling people to take risks and be creative in their work without fear of being embarrassed or ashamed.

The shift towards hybrid working has changed the nature of the psychological contract. Employers' and employees' expectations have changed, and a hybrid working environment, while more flexible, calls for greater trust and better communication to operate effectively. At the same time, employees are moving away from traditional demands for job security and towards newer demands for learning and development to improve long-term employability.

Navigating the opportunities and challenges

As with any change, hybrid working presents opportunities as well as challenges. Employers must work with their employees to understand both, and to come to an arrangement that is

inclusive of different individuals' needs. A key challenge facing organizations across the hybrid workforce is the impact of reduced face-to-face interaction and how this will affect employees psychologically and professionally.

Reduced time in a shared office space can limit opportunities for learning directly from colleagues. Employees working for prolonged periods at home can also experience loneliness and isolation, with fewer opportunities to socialize and build bonds with colleagues. The CIPD found that during homeworking in the Covid-19 lockdown, knowledge sharing and team relationships suffered.

On the other hand, hybrid working has many positives. The flexibility of hybrid working – and less time overall spent commuting – affords individuals more leisure time and greater capacity for caring responsibilities, wellbeing activities, learning new skills and volunteering. For some, including working parents, these benefits are the difference between a job being viable or not. Indeed, global EY research has found that more than half of employees would quit their jobs if not provided post-pandemic flexibility.

Yet, there is a risk for digital exhaustion caused by the increase of back-to-back online meetings. Work Trend Index 2022 reported that workday span for the average Microsoft Teams user has increased more than 13% (46 minutes) since March 2020, and after-hours and weekend work has grown even

“

Changes to the way we work do not affect everybody equally: working parents, women, neurodiverse individuals, and ethnic minorities may be disproportionately impacted.

more quickly, at 28% and 14%, respectively.

Crucially, changes to the way we work do not affect everybody equally: working parents, women, neurodiverse individuals, and ethnic minorities may be disproportionately impacted. For example, it is possible that those attending the office more regularly receive more facetime with managers, making their work more visible and potentially increasing the likelihood of promotion.

If this is the case, working parents, carers looking after relatives with medical and mental health conditions, as well as people from underprivileged backgrounds or lower socio-economic backgrounds, can be disadvantaged. For example, access to jobs in London with requirement to work on-site means budgeting hundreds of pounds for peak-time daily commuting.

Recently, BBC reported some concerns by Apple staff, who believe mandating working from office three days a week will make the company “younger, whiter and more male-dominated”. This negative impact could disproportionately impact women, who are still more likely to take on the brunt of childcare duties, and therefore more likely to make use of flexible working policies. Women are already attuned to the potential negative impact on their careers. Deloitte has found that, out of nearly 82% of women who experienced negative disruption from the pandemic, almost 70% feared that it might limit their career growth.

Work where it works

There is no single correct way for organizations to manage the shift in working patterns. We've already seen a variety of responses, ranging from companies that have swung back to an office-based culture to others who are embracing hybrid working wholeheartedly.

Google is mandating workers to return to the office three days a week in some US, UK and Asia Pacific offices. Goldman Sachs, similarly, expects a full return to the office. In contrast, Salesforce has introduced a new hybrid working policy. Part of its approach involves making provisions for preserving employees' health.

While some organizations have trialed a four-day working week without impacting salaries, a London law firm, Stephenson Harwood, provides an option to their employees to work remotely but at a cost: remote workers' pay will need to be 20% less than their current salary. Therefore, the debate will likely continue across industries, and negotiations between employees and employers will need to be handled sensitively as employees may be easily tempted to resign if their expectations are not met.

At NTT DATA UK, we have a ‘work where it works’ policy. If a person finds that they do their best work in the office, we have the facilities to support this. If they require flexibility and want to work from home, we can accommodate that too. The most

“

We need a strategic approach to the hybrid workplace and we need policies that will guard against the kind of inequalities that may arise from new ways of working.

important thing for us is to provide a system suited to individual needs.

As organizations formulate their strategy for work going forwards, it's crucial that the workforce is part of this process. Businesses must carefully consider the impacts on different individuals and groups. It's tempting to search for a one-size-fits-all approach and emulate it, but each business must focus on creating a working model that aligns with its own corporate values and purpose.

Following the pandemic, our working norms are still in flux as companies try to settle on approaches that bring the best of both remote and face-to-face engagements. This is an organizational transformation, and companies who use tools for managing effective business change will be better able to equip staff to make the most of hybrid working.

A hybrid working vision and roadmap should form a core part of any organization's communications plan. It's vital that this roadmap is clearly relayed to the workforce, and that all communication is based on empathy and an understanding of individuals' needs. We need a strategic approach to the hybrid workplace and we need policies that will guard against the kind of inequalities that may arise from new ways of working.

People lie at the heart of every organization,

and their wellbeing is pivotal to the success of the business. Having a collaborative approach to setting hybrid policies – with buy-in across all levels of the organization – can help build loyalty and promote a closer-knit community and culture that facilitates individual needs, and improves retention in the long-term. To ensure the wellbeing of the workforce, trust, empathy and transparency are key. With an approach founded on these principles, businesses and their employees can successfully navigate challenges and make the most of the opportunities available in the hybrid working world.

With thanks to the co-contributors of this article: *Miona Cvetkovic, Business Consultant – Digital Transformation & Change, NTT DATA UK, and Hannah Timson, Associate Consultant, NTT DATA UK.*

For references, please go to cxomag.com/article/nurturing-inclusivity-and-productivity-in-a-hybrid-world/



Pragya Limbu is a Principal Consultant for NTT DATA UK within Business Consulting. Pragya has worked across industries in travel, telco, retail, public sector and NGOs focusing on strategy, change and digital transformation. She is the

Deputy Lead for Business Change with a passion for technology for good, STEM and sustainability,

5 Minutes On...

Society 5.0

By Paolo Zanotti
Head of Marketing and
Communication, NTT DATA Italia



5 Minutes On... what role do organizations play in our new technological society and how should we approach the risks and challenges that come with it? We must be strategic and thorough in understanding how we can optimize technology as best as we can, while remaining savvy and careful.

Scan the QR
code with your
smartphone camera



Thriving When the “Authorities” No Longer Know What to Do

By Nick Craig, President of Authentic Leadership Institute and author of *Leading from Purpose*

Executives everywhere are having to re-evaluate their purpose and re-establish their resolve, building a new set of muscles to lead. True leadership is being the author of your own story, whilst staying true to your values. Holding on to that central purpose, that constant in a sea of changes, will allow leaders to thrive, even as the rulebooks are being rewritten before our eyes.

“It’s only when the tide goes out that you learn who’s been swimming naked.”

– Warren E. Buffett

The tide is going out and it really doesn’t look good these days. Whatever version of “authorities” that is supposed to be guiding us in this time doesn’t have a clear direction. Even Disney can’t escape the tide.

I know, as I am helping the C-suite in a number of organizations, they are humbled. Each executive is being required to find a place inside themselves they never had to before. They are building a new set of muscles to lead – and so can you.

Being the author of your own life

The key is to realize that at the core of the word “authority” is the word “author.” We are all learning in real time when it works to allow someone else to author our journey, and when we need to be in the driver’s seat.

Scary thought, isn’t it? Managing is about reading the manual and following it. Truly leading is about being the author and writing the story as you discover the truth. All of us are now here in this

“

**Managing is about reading the manual.
Leading is about writing the story as
you discover the truth.**

hybrid, post-Covid-19 (we hope), everyone-changing-jobs, adapting-to-agile-ways-of-working-and-living, Ukrainian-crisis, world. The word “author” is also at the core of the word “authentic”. That gives us a path to follow.

Fifteen years ago, I collaborated with Bill George to help launch the Authentic Leadership Movement. Much of what we discovered applies directly to the challenge of finding our authorship at this moment. And there is a new twist.

When I am working with leaders, I often ask them to create their definition of an Authentic Leader. Without fail, five notable characteristics emerge regularly:

1. The strength to show one’s vulnerability
2. Setting others up for success
3. Having a strong internal moral compass
4. Delivering sustainable long-term business results
5. A true sense of purpose.

Finding our authenticity

We find our authenticity and our authorship when we review some of the most challenging times in our lives. Often the moments in which we were the most challenged are the ones that provide the missing key. Leaders learn that on the other side of the journey into their own past, there is a deep well of insight waiting that only they can discover.

When we step back and unpack these events and how we turned the corner, the stories reveal a leader who had to author their path forward. These are stories in which our basic assumptions about who we are and how we relate to the world

are “reset.” We discover a level of resilience that we didn’t know we had. At some point, we lead ourselves out of the desert and into the Promised Land.

This is where you find your authorship in times of great uncertainty. It’s all within you: you will need to dig deep and connect to those times when there was no map and how you then made it out. This is what I find myself doing a great deal with leaders these days.

The new twist is how central purpose has become to the process. In a world in which nothing is the same, we all need something that doesn’t change. The deeper purpose that drives you is the one thing I have seen that doesn’t change. Purpose is the unique gift that you bring to the world. It is the underlying source of your authorship.

The key question is: if you disappeared tomorrow, what would be desperately missed? Most of us don’t know the answer to this fundamental and critical question. It is truly humbling to a multitude of leaders I work with to realize that something so basic is so unclear to them. And that lack of awareness shapes the manner in which they lead. The impact of knowing in your bones what purpose has been driving you, and what leads you when all else fails, is the most important ingredient to being the author and mapmaker in this moment.

How to thrive, not just survive

I recently worked with a leader, Vincent, who was deeply challenged. Vincent had just kicked off a company-wide rollout of agile working to more than

“

**Often the moments in which we were
the most challenged are the ones that
provide the missing key. Leaders learn
that on the other side of the journey into
their own past, there is a deep well of
insight waiting.**

10,000 employees. It had been three years in the making, and this was to be his finest hour. Yet, on the launch date, he discovered that someone else had been hired into the company with the same qualifications and experience to do his job, by his skip level boss.

As we talked, we realized the easy answer would be to quit. Yet his purpose wouldn’t let him. His purpose is to “make it so.” He is the leader who, when things look impossible, pulls the team together and co-creates a course of action that turns the problem into a triumph (just like Jean-Luc Picard of the starship Enterprise!)

As we sat there, I could see two parts of him: the part that was crushed and just wanted to run, versus the leader who makes it happen. We all have these two parts of us, but most of us have not fully defined our voice of authorship, our purpose. Vincent, through looking at the most challenging times in his life and how he thrived versus just survived, had authored a journey that turned a threat into an opportunity.

Through dialogs with his boss and the new hire, they began to create a path forward that leveraged each of their gifts and helped address how to apply agile to 30,000+ employees. In addition, Vincent was asked to run the company’s response to the Ukrainian Crisis. Having a large portion of business in Russia, this role is probably the most visible and important task in the company at this moment. Who better to run it than the leader who “makes it so?”

Stepping into his purpose, Vincent has changed ways of working and leading. The company’s daily

review meetings have gone from just 10 people attending to more than 150. Why? Because Vincent runs the sessions with a combination of humor, collaboration and focus unlike anyone else. He learned to embrace the fact that, while someone else has the same qualifications as him, it is his purpose – his unique gift – that he alone has, which sets his authentic leadership apart.

Now that purpose has shown up, the “authorities” know that Vincent is the leader who can help them thrive when it matters most.

For references, please go to cxomag.com/article/thriving-when-authorities-no-longer-know/



Nick Craig is President and Founder of the Core Leadership Institute (CLI), which works with leaders around the globe to deliver transformational development programs. Originally the Authentic Leadership Institute, CLI has

expanded its focus from authenticity to purpose. Nick is author of *Leading From Purpose*, co-author of *Finding your True North: A Personal Guide* and the 2014 Harvard Business Review article *From Purpose to Impact*. This year, Nick launched the “Leading From Purpose” podcast series and created an alumni community for CLI.

Trusting the Human in Our Future

By Philipp Kristian, Human Futurist, author of *The Trust Economy* and *RESET*

Employees and customers have new expectations of organizations, not just to speak and understand their language, but ultimately to be human – in the decisions that they make, the values they represent, and the way they contribute to human progress. Trust is the driving force of change and value creation; trust gives us the power to reimagine, rethink and reshape our world, environment and professional as well as personal context.

“

We must shift our focus from the outputs that we innovate to the outcomes that make an impact. It becomes not just about what we do, but how we do it.

Many of us intuitively recognize trust as an emotion – a necessity, and something good and valuable. But when we appreciate trust beyond that – specifically, its role shaping how we operate as a society and what this means for the organizations that we’re a part of – we begin to understand just how pivotal it really is. Trust is central to global human progress; to how we’re interacting, collaborating, and growing as people. It’s time to amplify and hone that.

In much of my previous literature, including my books *The Trust Economy* and *RESET*, I explore how trust makes the world that we’re creating. Much of this delves into how we integrate trust into the digital and physical interfaces that we create for our customers and people. How trust begins as our imagination of the future, and materializes in the opinions we hold, decisions we make, and actions we take. And while these are significant indicators of an organization’s ability to make it or break it in today’s world, a much bigger picture has come to light over the past two years. Trust is but one part – albeit a critical part – of that picture.

Now, we must explore how we humanize our organizations from the inside-out and outside-in. In this way, we shift our focus from the outputs that

we innovate to the outcomes that make an impact. It becomes not just about what we do, but how we do it.

So, how exactly do we do it?

Levels of trust

Let’s begin with the basics. There are different levels to trust. Grasping trust in this way helps us analyze at which level we’re playing, and how we can improve going forward.

Many companies naturally operate on the first level of trust: **transactional** trust. It’s the hygiene factor – the preconceived notion that it’s secure and safe. It earns you a right to join the party, but it means you are one of many.

The second level of trust – one that I think many companies are aspiring towards – is **expert** trust, i.e. being driven by innovation, ahead of the curve and cemented as an industry leader.

What organizations should really be oriented towards is reaching that third ultimate level of trust: **universal** trust, i.e. no matter what, as a customer, I trust you unconditionally because I believe in what you’re doing. Apple is a perfect example of this. Generally, consumers take the universal trust at face value, believing that what the company makes is

“

Trust enables the large complex collaboration systems that humans have evolved over time. That’s our true human superpower.

going to be good.

If universal trust is the aspiration, let’s consider this equation as a modus operandi:

Behavior = motivation × ability × trust

How we’re engaging with the world is determined by our willingness to do it (motivation), whether we are actually able to do it (ability), and the degree to which we put trust in our motivation and ability to proceed. When we have zero trust, very little happens. It means trust isn’t everything and yet, in its absence, everything becomes nothing.

More often than not, our motivation and ability are directly correlated to our trust in others and trust within ourselves. Distilling this concept into three key points:

1. Trust is the driving force of change and value creation; it’s about directing behavior in a new way.
2. Trust is the enabler for collaboration. Try collaborating with someone that doesn’t trust you. It’s a deal-breaker. Trust enables the large complex collaboration systems that humans have evolved over time. That’s our true human superpower.
3. Trust is a neutral power. It’s never just about

trust. It’s about what we do with that trust. Trusting ourselves is enabling our very own leaps of faith, as leaders of ourselves, of organizations and of others. It’s trusting something new and trusting ourselves to do something different that is driving innovation and change for the better.

The basis for a culture of transformation

Building on that final point, trust itself is simply a catalyst and force for new things. That makes it neither good nor bad. It’s simply an emotion influencing our behavior for better or worse. Trust gives us the power to reimagine, rethink and reshape our world, environment and professional as well as personal context.

It’s empowering us to act with agility in times of change, to flex with the requirements and to embrace every uncertainty we encounter as an opportunity for inspiring something extraordinary. It’s a force we can use to heal the issues we most need to change and emerge as a better humanity.

That’s why trust matters, to me, to you, and to everyone around us. Trust is key to a culture of transformation, and to transformation of culture. It’s in everyone’s best interest to put this on top of

“

The first and most rudimentary basis for trust is simplicity. It really comes down to how you create an experience that diffuses complexity.

the agenda globally. The first and most rudimentary basis for trust is simplicity. Inherently, it's easier to trust simple things. There's a problem around complexity, which distorts and distances customers from trusting brands. At the rudimentary level, it really comes down to how you create an experience that diffuses complexity and sets a clear outcome for all involved. Now that's just the base.

Once you have a simple system, you must then consider how you infuse organizational purpose. Why should I go with you? What's the differentiation and how do you explain it to me in a credible story? How can you be a bit more original and authentic? When you champion a vision worth buying into, your people and customers intrinsically begin to trust you. When they do, they will champion you and, in turn, you will inherently do right by them. We've seen a lot of companies reevaluate and reinforce their purpose over the past decade – and we've also seen the difference it's made in their ability to survive the changing tides.

The human in our future

This brings us back to my earlier and most central takeaway: our future – and the future of our organizations – depends on humanism. Our people and customers not only expect organizations to speak and understand their language, but to

ultimately be as human as we are – in the decisions that we make, the values that we represent, and the way that we contribute to human progress.

Indeed, trust is the imperative that rests across all three of these planes. As we are embracing the challenge, opportunity and expectation of transforming humanity for the better, we must begin by transforming our own humanity. This means growing into our own greatness as leaders and organizations for good. In this case, how it's all going to unfold – well, that's resting in our hands.

For references, please go to cxomag.com/article/trusting-the-human-in-our-future/



Philipp Kristian is a TEDx keynote speaker and human futurist. His C-level interventions as a thought leader, innovation strategist and executive educator embrace the philosophy of less-is-more and feel almost surgical. His deep expertise draws on over a decade of driving innovation and leadership transformation across blue-chips in JAPAC and building the future with the Founder/CEOs of major digital disruptors. His books, *Reset* and *The Trust Economy*, humanize our take on digital trust and post-pandemic future.

5 Minutes On...

Building Technology Around Human Needs for Trust

By Philipp Kristian

Human Futurist, author of *The Trust Economy* and *RESET*



5 Minutes On... why trust is no new concept. It is a human emotion and principle that is in a renaissance in light of the digitally evolving world we exist in. It is the glue that combines productivity and collaboration without losing the human element. We must build technology around human need, not the other way round.

Scan the QR code with your smartphone camera



The Purpose-Driven Corporate: Reimagining the Power of Business

By Debbie Haski-Leventhal, CSR expert, professor of management at Macquarie Business School and author of *Strategic CSR: A Holistic Approach to Responsible and Sustainable Business*

In the last decade we have seen a genuine move towards a more holistic approach to the role of business in society. When we use who we are and what we know to serve others, we create a sense of meaningfulness that increases happiness, connectedness and impact, both on a personal and organizational level. And when companies decide to walk the talk and lead with purpose, there is no limit to what can be achieved.

In 2000, Unilever acquired the ice-cream company Ben & Jerry's. Known for its social mission and holistic approach to business responsibility, its stakeholders criticized the move, saying that Ben Cohen and Jerry Greenfield 'sold out'. Unilever, a multinational consumer goods company with dozens of brands, was not conceived of as a good company by many of Ben & Jerry's followers.

However, in 2009 Paul Polman became Unilever's CEO and changed the business for good. He led its Sustainable Living Plan, became an influential actor in the UN Global Compact, and used the company's power to help design and achieve the Sustainable Development Goals (SDGs). Employee engagement increased, consumers became part of the transformation, and its share prices nearly doubled under his leadership. Nonetheless, Polman always said that quarterly reports could not achieve the world that we want. We need a long-term vision for business to become a force for good.

Why CSR became essential

The last decade witnessed a global shift in the

business mindset. If in the 1970s it was believed, as Milton Friedman asserted, that 'the only social responsibility of a business is to its shareholders', the 1980s and 1990s saw the rise of corporate social responsibility (CSR). Still, it was perceived narrowly as a marketing and sales strategy, focusing on philanthropy and cause-related marketing. This approach led to unethical shortcuts and greenwashing.

When CSR is only implemented for financial gains, it can be done superficially. It was dangerous, with companies like Enron having CSR reports and not much action to support it. It was as if many companies and business leaders missed the true meaning of the word 'responsibility' in CSR. Distracting everyone with some dollars for charity, companies continued to trash the planet, increase modern slavery and devastate local communities.

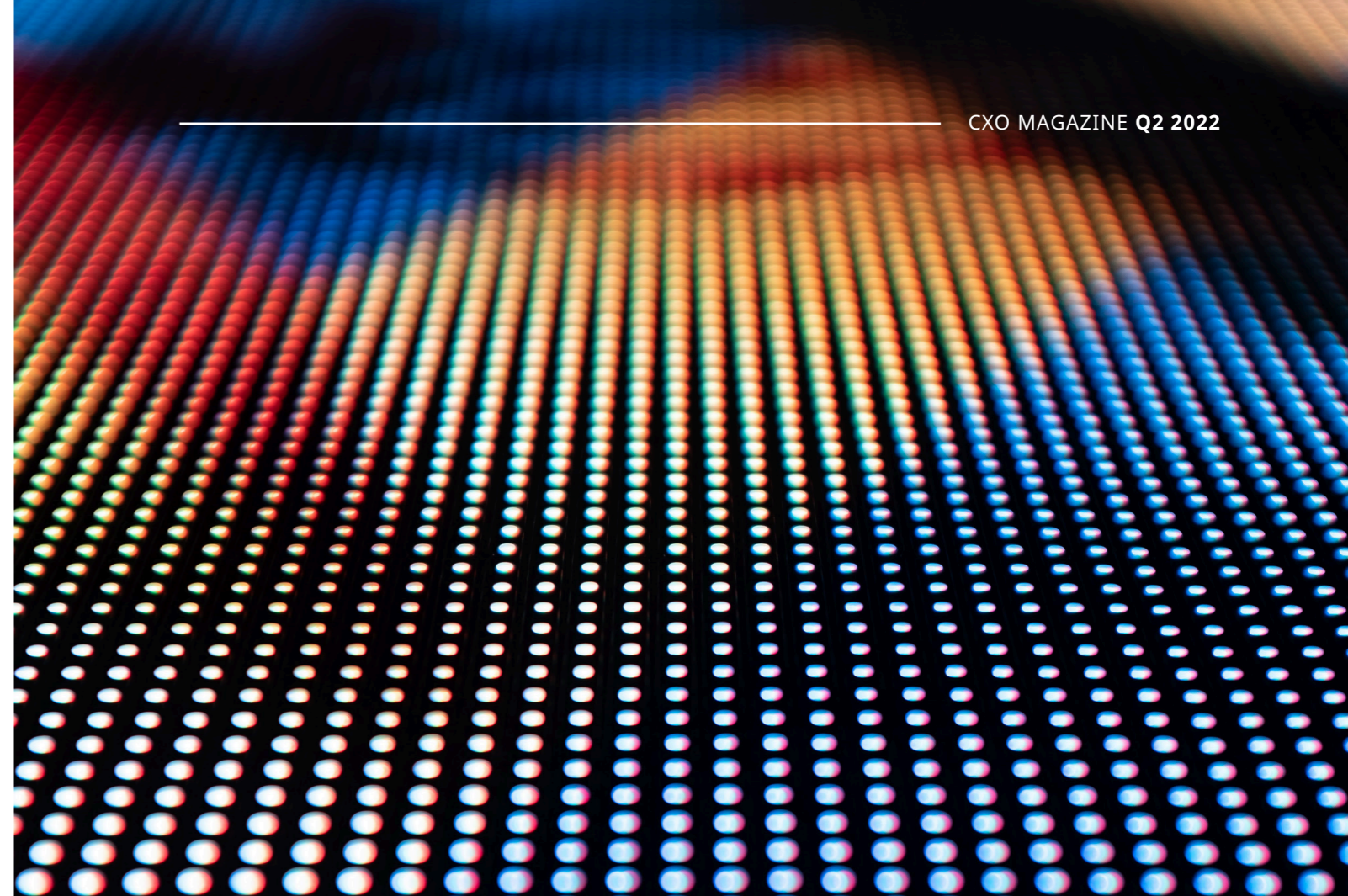
It is only in the last decade that we truly see a movement towards a more holistic approach to the role of business in society. In 2019, the Business Roundtable released the Purpose of a Corporation, which affirmed a shift in its nearly-200 member

CEOs' commitment to a broader set of stakeholders. Companies began to apprehend that CSR is not a sideshow, a nice-to-have aspect of the business; but at the core of the business, embedded in every part of its value chain.

In my book, *Strategic Corporate Social Responsibility*, I define it as 'a holistic and long-term approach to the broad responsibilities of business, based on stakeholder integration and ethical behavior, while utilizing the firm's resources and brand to address societal and environmental issues.' It incorporates every part of what I see as 'responsibility' – a holistic approach, long-term thinking and ethical behavior.

Seeking our purpose

However, we now need to take it one step further and move to the next level of purpose. Purpose is the reason for which something was designed. If you look around you, every object in the room was created for a reason. When objects can no longer serve their purpose, we deem them 'broken' and terminate them. Yet, the purpose of a person or a



“

It was as if many companies and business leaders missed the true meaning of the word ‘responsibility’ in CSR. Distracting everyone with some dollars for charity, companies continued to trash the planet.

company is more complex. As humans, we are not created for a specific purpose, and we need to seek it.

In my upcoming book, *Meaningfulness*, I assert that we find purpose by tying our talents and skills with our passion and joy to generate a positive impact around us. A lawyer passionate about domestic violence can use her talent to work pro-bono for abuse survivors. A yoga teacher who cares deeply about refugees opens a free yoga center to help these communities. When we use who we are and what we know to serve others and help, we create a sense of purposefulness and meaningfulness in our lives. This, in turn, can lead to higher levels of happiness, health, connectedness and impact.

It is not too dissimilar to the organizational-level process of a purpose-led company. While some companies like Ben & Jerry’s were created with a vital social purpose, others, including Unilever, ascertained it later. Patagonia was founded by environmentalist Yvon Chouinard to demonstrate how businesses can sell products while still aiming to save the planet.

Companies establish their purpose by connecting who they are and what they know to the impact that they can create. Some, like Starbucks, realize that they have an immense opportunity to make a difference simply by deciding on a more inclusive

hiring policy. Others change their mission statement and approach to harness their power, resources and talent to make a difference in society.

When LEGO decided to be a champion for gender equality, it changed some of its products and ads to push this agenda. Airbnb used its campaign to promote LGBTQ+ rights and social acceptance. Google leverages its vast amount of renewable energy to help one billion people live more sustainably. It is also done through small actions, such as adding the carbon emissions on Google Flights. A positive organizational purpose is most powerful when tied to the impact the company makes by harnessing all its resources.

When companies decide to walk the talk and lead with purpose, there is no limit to what can be achieved. It is no longer about giving money to charity to patch over negative actions elsewhere. Donating a dollar from each garment made using modern slavery and child labor is no longer acceptable.

Taking a holistic approach, mending the value and supply chains first, and utilizing the power of business as a force for good is the only way forward. We can achieve the SDGs, such as no poverty and zero hunger, by 2030 if all the multinational companies pay people liveable wages everywhere. It takes a solid purpose, goodwill and responsibility.

“

One of my studies showed that 95% of business students would sacrifice some of their future salary to work for an employer who cares for all stakeholders. Pay them well too, and you win the war for talent.

Purpose-driven organizations are more comfortable with social, political, and climate activism because they are seen as companies who care.

The rewards of a purpose-driven life

When people live a purpose-driven life, they reap the positive outcomes mentioned above. When companies do this, their employees are more engaged and committed, centered around a solid value congruence and purpose alignment. It provides workers with a sense of meaningfulness which can have a ‘spillover’ effect on their lives.

This is particularly important in the face of what is now called ‘The Great Resignation’. Young employees seek to work in purpose-driven companies. One of my studies showed that 95% of business students would sacrifice some of their future salary to work for an employer who cares for all stakeholders. Nearly one in five were willing to forgo more than 40%. Pay them well too, and you win the war for talent.

When companies walk the talk and truly live by their purpose, they also generate trust among employees, consumers and stakeholders. Trustworthiness is such an important currency in today’s world, and although not many companies are trusted on their ethical behavior, this can change with a new discourse, ethos and action.

People desire to find their purpose, live a more purposeful life, and work with and for purpose-driven companies. Business leaders will do well by reimagining the power of business to do good in the world, (re)define their ‘why’ and work with others to not only increase shareholder value, but societal value too. It is the only way forward.

For references, please go to cxomag.com/article/the-purpose-driven-corporate-reimagining-the-power-of-business/



Debbie Haski-Leventhal is a Professor of Management at Macquarie Business School and an expert on corporate social responsibility (CSR), purpose, and volunteerism. She is a TED speaker and a public speaker on purpose and social responsibility. She has published over

60 academic papers, and her work was covered by the media, including The New York Times. Haski-Leventhal is the author of *Strategic CSR: A Holistic Approach to Responsible and Sustainable Business*, *The Purpose-Driven University* and *Employee Engagement in Corporate Social Responsibility*. Her new book, *Meaningfulness*, will come out with Simon & Schuster next year.

People-Centric Banking: How to Gain the Trust of Future Generations Through Sustainability

By Gianluca Randazzo, Head of Sustainability, Banca Mediolanum

As one of our oldest institutions, banks have a pivotal role in shaping our local communities and even our global society. Going beyond being customer-centric, some banks are embracing being people-centric – looking after and enhancing the community they serve. By placing sustainability at the core of their strategic practice and relationship building, banks can build trust with all customers, and in particular the younger generation.

Worldwide events have influenced all kinds of aspects of the lives of those who have grown up through them. Just as the financial crash of 2008 influenced the spending habits of Millennials, the Covid-19 pandemic has clearly shaped those of Generation Z. Covid created a financial disaster for many globally, and while it wasn't the catalyst for sustainability awareness, it certainly drove Generation Z to feel the impacts and drive its importance forward, being the first to raise any red flags if their expectations are not met by businesses today.

These expectations are increasingly setting the standard for consumer expectations in ethical retail and consumer behaviors. The spending power of Generation Z (those born since 1997) and Millennials (those born between 1981 and 1996) is not to be underestimated. Gen Z makes more shopping decisions based on sustainable retail practices than any other generation. Therefore, commercial strategies must be human-centric; we must be sustainable in every area of business, from reducing our carbon footprint to building long-term,

genuinely-supportive customer relationships.

Nowadays, sustainability is louder in actions than ever. At Banca Mediolanum, we aim to provide young people with greater control over their finances, so we must prove our sustainable practice to build their trust, which in turn brings us business results from the trust we have created. You can say whatever you want, but you will be judged immediately from the actions you take. If you are found to be insincere, or worse, knowingly discriminatory or damaging, you will soon feel the loss in your bottom lines.

Our strategy for the Net Zero journey

Being zero impact in financial business is difficult. We can offset our emissions through where we work – such as working from home and saving emissions from travel, and sustainable management of our buildings – but when it comes to investments in other assets and company shares, it is difficult nowadays for anyone in the world to say they're 100% zero impact.

Instead, we are on a journey. We are really

committed to the idea of being helpful for the people we meet, who become our customers and our community, so we are on a journey to be responsible for them because we know that we are part of that community.

We cannot forget our responsibility and forget where we are. This is something our founder wanted to share with other people working for the bank, which has become our ethos.

You can see this in our strategy, where we work around four pillars:

- **Economic responsibility** – because we are a bank, we are responsible for everyone. We can be ethical and profitable, solid and liquid. We can be political ambassadors. If we are profitable, we can pay salaries, employees and the community.
- **Customer responsibility** – we don't exist if customers don't choose us. Not just to answer their needs, but to help them. The right products, and making sure those products are as sustainable as possible.
- **Communication** – keeping close to customers

“

You can say whatever you want, but you will be judged immediately from the actions you take. If you are found to be insincere, or worse, knowingly discriminatory or damaging, you will soon feel the loss in your bottom lines.

with the right communication at the right time, and always acting transparently. Any kind of communication must help the customer to understand how things are going, why they are receiving particular financial advice, and what they should do with that information.

- **Employee experience** – making sure people feel comfortable working for us. Services, taxes, salary, experience, childcare – these are part of the employee experience to get the best from any of us inside the company. Everyone has a talent, and we have to give them the chance to let the talent shine, for the betterment of the individual and the community. Employees want to work for a company that has a purpose, which embraces diversity and has a positive impact on the environment, so we need to meet those expectations.

Building a sustainable identity

We are not 100% sustainable, but we are committing to building a sustainable identity through philanthropic abilities and CSR efforts, and our path is mostly defined already to achieve our goals.

In 2021, we carved out 860,000 hours of training for 4,800 employees, roughly 100 hours of education per person. We can't say we are sustainable; we have to be sustainable. As our CEO outlined in our principles, we are part of a community, so we can't forget it. From a business point of view, if the

community we find ourselves in is growing, we have more opportunity to grow with it; if we don't know the people of that community, they won't know we exist.

Every year we give €3.5 million to projects in Italy and all over the world. We also offer free financial information on anything, from how to use money to what a debit card is, helping students, young people, or immigrants who arrive in Italy to find a job, with their financial education. We are trying to help educate as well as innovate. To attract and relate to young people, we used an influencer campaign, using influencers we researched that the general public actually liked, which brought us new business.

From an environmental point of view, we are trying to reduce emissions where we can. We do this by trying to use electricity from renewable sources and focusing on our investments, measuring our impact and looking at solutions to be effective in reducing our impact. For a financial institution, it is a long journey. It should be quicker, but of all industries, the financial industry is difficult to change.

Much of our digital products are intended to inspire healthy and green activities to unlock rewards for clients, which both promote sustainable habits and win business. In turn, we continually assess how we can be as sustainable as possible in practice.

“

From a business point of view, if the community we find ourselves in is growing, we have more opportunity to grow with it.

Our new challenger bank, Flowe, was born from the idea that it is possible to be sustainable with human centricity. It is the kind of bank where you can find all the details about how to live better. It has videos to advise with environmental info and how to live a more sustainable life physically, mentally and environmentally for the next generation, but also to inspire better living across all generations.

The Flowe Card is a wooden debit card. When you request it, we plant a tree in Guatemala to offset carbon emissions to support the local community there. In the first year of its introduction, we planted over 38,000 trees.

Reaping the rewards of trust

Being sincerely committed to sustainability brings trust, which generates value for business and society. If you really are committed to these values, you build an identity that customers will recognize. We want people to know our commitment to giving our best.

After publishing our non-financial report which outlined our ESG efforts, we noticed a positive peak in stock prices for Banca Mediolanum. While this may not be directly correlated, it does suggest that publicly shared results increase transparency and trust.

We aim to be culture shifters and influencers, always developing projects with sustainability in

mind. Consumers are changing their demands, so our offering must change with them, by building a fully digital banking service that aligns with Generation Z and Millennial needs and values.

How you approach this topic can build a very different relationship with customers, which generates different outcomes. You can keep it business based, which is functional. But if you prioritize people as much as you prioritize business needs, then you will also attract customers that value that commitment – growing your business, and increasing the positive impact you can have in your community. If you put the person at the center, everything will change for the better.

For references, please go to cxomag.com/article/how-the-circular-economy-benefits-business-and-investors-while-tackling-global-challenges/



Gianluca Randazzo has overseen sustainability-related development for the Mediolanum Group for over 25 years and supports the Board of Directors in designing and implementing sustainability strategies, handling stakeholder relationships, promoting and coordinating environmental projects, drawing up the non-financial statement and organizing activities of Fondazione Mediolanum Onlus. He is a board member of the Management Committee of Fondazione Italia Sociale, the Board of Directors of Fondazione Mediolanum Onlus.

Digital Trust: The Difference Between Future-Fit and Obsolete

By Noel Chinokwetu, Security Consulting Senior Manager, NTT DATA UK and Charanpreet Aulakh, Senior Cybersecurity Consultant, NTT DATA UK

Ignore digital trust at your peril. Customers are talking with their feet, cutting ties with brands that display poor data security. The essential ingredient, in this age of digitization and mass data collection, is unwaveringly strong cybersecurity.

The last decade has seen an unprecedented surge in the need to amass vast amounts of client data and most interestingly, a sharp increase in the value of consumer data to the business, as digital enterprises rely more and more on data collections for profitability and growth.

As organizations grow and data pools expand, so does the associated cybersecurity risk (and so too does the need for improved risk management approaches). Risks to the security of consumer data range from deliberate actions of cyber criminals to inadvertent disclosure or loss through employee actions. Whether in a B2B or a B2C scenario, data security should always take priority.

What is digital trust?

Digital trust is the established relationship built on confidence that an organization is able to safeguard its collection of consumer data, information assets and technology resources. Many authorities have different views on how trust is achieved. We have come across assertions like ‘trust is granted’ or ‘trust is earned’, but for me, the great American scholar



Ralph Waldo Emerson summarizes it all: “Trust men and they will be true to you; treat them greatly and they will show themselves great.”

He was right, trust is reciprocal. It is classic quid pro quo (‘something for something’ – or ‘you scratch my back and I’ll scratch yours’). In simpler terms, all consumers need guarantees that their data is safe before they can comfortably share it.

Demonstrating trustworthiness

Research done in the past has shown that consumers are overly concerned with data security and privacy. For example, The State of Digital Trust Data Report from February 2021 by Okta states that 42% of Americans and 47% of UK respondents say data mishandling or selling would cause them to lose trust in a brand.

The report concluded that “when it comes to building trust, consumers care most about the core competencies: service reliability, strong security, and good data handling practices. Survey respondents also made it clear that trust in our digital world directly impacts purchase decisions,

and many cut ties with untrusted brands altogether.”

While trust is reciprocal, it is the data collector who must strike first. In a B2C scenario, this would be the business and in a B2B scenario it would be the service provider. Bolstering digital trust entails using cybersecurity as a key enabler.

The primary focus should not only safeguard privacy, confidentiality, integrity and safety aspects but extend to ethical aspects as well. It is all about taking actions that boost confidence and subsequently encourages sharing of data, like demonstrating security and transparency. As an example, to demonstrate transparency to customers, Microsoft releases biannual digital trust reports. These reports consist of the Law Enforcement Requests Report, US National Security Orders Report, Content Removal Requests Report and Digital Safety Content Report. The reports detail what information has been shared, with whom, and how many requests have been accepted or denied, among other things. This demonstrates a continuous effort to provide customers with visibility and control over their data, whilst at the same time

“

47% of UK respondents say data mishandling or selling would cause them to lose trust in a brand.

enabling the organization to make informed choices and strive towards building and maintaining trust in technology.

Clear ways to build greater trust

Demonstrate transparency: Transparency is critical for building trust and loyalty. This includes the disclosure and provision of an end-to-end view of what consumer data is used, and how it is used, processed, transitioned and retained.

Constantly engage consumers: Beyond consumer transparency, the engagement with consumers enables us to build good working relationships, for example to establish how best to improve services, in terms of securing their data and accommodating their needs. Periodic surveys are an effective way for gathering consumer views.

Act ethically: Act honorably and with integrity. Use data for the sole purposes that it was collected. An organization's integrity and reputation are essential to maintaining trust. This extends to using technology responsibly, for example when using artificial intelligence to draw insights from data sets, ensure that the analysis is carried out within the defined scope and avoid drawing insights that the consumers may not be comfortable sharing.

Comply with the law and regulations: Abide by the governing legal requirements applicable in the jurisdictions that the organization operates in. Regulations such as GDPR / Data Protection Act of 2018 need to be satisfied, and assurances for continued compliance shared with the consumers and data owners.

Continuously improve cybersecurity: Providing comprehensive cybersecurity protection is vital to bolstering digital trust. Getting accreditation and third party assurance is a good way to demonstrate best practice. Here are some key cybersecurity security principles for maintaining secure data protection environments:

- **Drive cybersecurity through strategy:** Creation and implementation of clear, business-aligned and fit-for-purpose cybersecurity strategies is key. Technology is not always the answer; some issues just need a governance procedure or strategic steer. Strategy ensures selection of right technology solutions to solve business specific cybersecurity problems.
- **Practice cybersecurity hygiene:** Reduce the organizational vulnerabilities by identifying risks and deploying mechanisms to reduce or resolve risks identified, for example adopting

“

Act honorably and with integrity. Use data for the sole purposes that it was collected for. An organization's integrity and reputation are essential to maintaining trust.

a good practice aligned malware protection strategy.

- **Encrypt your data:** Encryption is an effective way of maintaining data integrity and confidentiality. All data such as mission-critical data and personally identifiable information (PII) should be encrypted at rest, in transit and where technically feasible, in use.
- **Automate where possible:** automation of data processing lowers risks of exposure and human error.
- **Standardize and benchmark your security controls:** Adopt tried and tested good practice frameworks such as ISO27001, NIST Cybersecurity Framework, Center for Information Security (CIS) and Information Security Forum (ISF), to name just a few. This allows auditable security controls that organizations can use as attestations of the adequacy of their cybersecurity arrangements.

As technological development increases in our digital age, cyber risk and security threats increase in tandem. But by increasing digital trust through robust cybersecurity, organizations are able to not just protect themselves and their own futures, but the safety and loyalty of their customers.

For references, please go to cxomag.com/article/digital-trust-and-cybersecurity/



Noel Chinokwetu is a cybersecurity professional with a wealth of experience and expertise in security governance, risk and compliance (GRC), security assurance and cloud security across various industrial sectors.



Charan Aulakh is a Senior Security Consultant with over six years of experience across multiple industries, with a keen interest within governance, risk and compliance (GRC).

Earning Trust and Customer Capital Through Integrity

By Ilenia Vidili, Customer centricity advisor, keynote speaker and author of *Journey to Centricity*

Trust is what defines a business. To gain the utmost respect of not just their customers, but their employees, partners and communities, companies must earn their trust. But earning high levels of trust from people external to the business must begin with an internal commitment to integrity.

“

The challenge is to curate trust as well as the balance sheet, and the opportunity is to fill the voids in trust that governments and institutions create.

Companies across the world have been establishing their prominent and solid presence since the first Industrial Revolution. Size was not only a symbol of business success, access to capital and market share, but also one of trust. Trust used to flow upwards, to CEOs, institutions, brands and governments. Unfortunately, this type of trust is widely viewed as steadily declining on account of violation of the social contract – corporate wrongdoings, government corruption and misinformation.

Previous experiences have shown time and again how fragile organizational trust can be and how serious it is when it vanishes. As a result, trust flows sideways – to colleagues, peers, influencers, bloggers, strangers and smaller shops instead.

When trust erodes, it's extremely difficult to repair. It creates disappointment and disengagement among stakeholders: customers, employees, suppliers and communities.

However, stakeholders have reported higher levels of trust in businesses since the pandemic, which is attributable to the positive actions that many companies made during the outbreak. They have experienced that ‘the business of business’ can be good, but a little good behavior from the past doesn't guarantee the protection of progress in the future.

This poses both a challenge and an opportunity

for business leaders. The challenge is to curate trust as well as the balance sheet, and the opportunity is to fill the voids in trust that governments and institutions create.

There is a common misconception in the business community that a brand can build trust. Believing that trust can be built implies that brands are in control. But brands earn trust by demonstrating consistent trustworthiness. So businesses should work towards continuously earning trust as the essential ingredient for strengthening relationships with stakeholders.

And why is there so much fuss about earning trust? Because stakeholders will be more loyal, more engaged, and be true advocates of the brand.

The main problem, however, is the disconnection between how business leaders and stakeholders believe trust is earned. Business leaders think emphasizing their product or service earns trust. Stakeholders think emphasizing integrity earns trust. Neither of these factors on its own is enough: brands need both. Here are three ways in which brands can earn trust through integrity.

1: Leading with integrity

Trust is rooted in a company's integrity; in other words, how a company's values come to life through its actions. But brands don't have values as such;

their people do. Much of how companies earn trust is tied to how their leaders behave. Our actions as business leaders are central to our integrity, but stakeholders are the ones who assess this integrity on a daily basis and rely on those actions.

There is one thing that can help in achieving this: alignment. Employees can feel that alignment, live the values and become brand ambassadors by continuously checking:

- Are our promises aligned with our commitments?
- Are our values aligned with our actions?
- Are our values aligned in the face of adversity?

Alignment also means that we actually ‘walk the talk’, rather than just putting a brand promise out there and expecting others to take action. People in high-trust companies reported 106% more energy levels at work, 74% lower stress and 76% greater engagement. This will organically radiate trustworthiness to customers.

2: Integrity beyond profits

As faith in institutions continues to spiral, stakeholder expectations are on the rise. Trust can be earned when we align our integrity to our purpose and then deliver on it, over and over. According to the 2022 Edelman Trust Barometer, respondents want more business engagement in society, not less.

It's believed that businesses are not doing enough on climate change (52%), economic inequality (49%) and trustworthy information (42%). As we are driving into the Fourth Industrial Revolution, stakeholders expect business leaders to play a bigger role in society than just running companies.

New generations of consumers and employees increasing their buying and staying power expect companies to have a purpose beyond profit. In order to earn long-term trust, business leaders must focus on long-term thinking that goes beyond maximizing shareholder value. As I set out in my recently released book, *Journey to Centricity: A Customer-Centric Framework for the Era of Stakeholder Capitalism*, “As ethical business conduct gains prominence as a means to evaluate the authentic trustworthiness of a brand, profit alone is no longer the sole measure of a company's success.”

3: Integrity beyond products

It's believed that consumers only look at rational factors like product price and quality. Yet, we human beings base our decisions to trust brands on emotions and feelings too. This doesn't mean that the public doesn't care about the company's offering. Trust is not earned from the product alone but from the culture in which the company delivers that product.

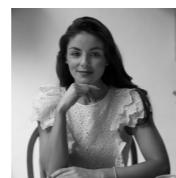
“

We human beings base our decisions to trust brands on emotions and feelings. Stakeholders don't just care about what companies are selling, they care about why and how they are selling it.

Trust tends to break down in situations where there is misalignment. Misalignment happens when the gap between promise and actions widens. For example, if a company promises to “improve the individuals’ quality of life through natural products”, but the people picking the raw ingredients work in poor conditions, that’s going to create a huge trust gap.

As business leaders, we should be continuously asking: does my product deserve my customers’ trust? Stakeholders don’t just care about what companies are selling, they care about why and how they are selling it. In fact, 81% of consumers said that they have to trust a business before they buy from it.

It’s worth remembering that every business is unique and there is no one-size-fits-all approach to earning trust. However, there is one common principle: the commitment to earn, re-earn, and maintain stakeholder and society trust for the long term. Some businesses may be able to succeed in the short term without strong trust foundations. But a business without trust will eventually lose its social license to operate.



Ilenia Vidili is a passionate customer-centricity advisor, author and keynote speaker. Driven by bringing humanity to business, her mission is to see a brighter future, where companies embrace a higher purpose, create value for all stakeholders, and contribute positively to society. She is the author of *Journey to Centricity*.

For references, please go to cxomag.com/article/earning-trust-and-customer-capital-through-integrity/

In Depth

NTT DATA takes a deeper look into critical areas of business trust.

Zero Trust: Your Digital Transformation Requires a Risk Transformation

New and evolving technology landscapes need evenly-matched cybersecurity: as new opportunities arise through digital tools, so too do new risks. Using a framework such as Zero Trust – which assumes every entity attempting to access the system or network may have malicious intent and therefore, as a default, should not be trusted – provides the visibility and controls needed for modern businesses to protect themselves and their customers.

Scan the QR code with your smartphone camera



Ethics: A Consultant's Guide

By Ian Bower, Director, Business Design Lead, NTT DATA UK

Being able to recognize a consulting organization's ethics, reflected in their culture, greatly influences their clients' ability to trust them. It is therefore the remit of the individual consultant and the organization to ensure they are engaging clients with the best intent, that they don't falsely represent themselves, that they charge fairly, and conduct their business with integrity.

Ethics in professional consulting is not always the first thing on the organizational agenda. But, having been described as there to help 'identify and solve managerial and operating problems of the various institutions of our society', consultants are bestowed with a considerable amount of trust and responsibility. Ethics should therefore be at the forefront of any professional consultant's (and their firm's) minds and actions.

Not all situations lend themselves to being easy ethical decisions. In the past, I have found myself having to question the actions or requests of others from time to time, whether it is on a piece of work we are delivering, how we are selling work, or our approach. At times we could find a conflict in what we are contracted to deliver and the "next piece of work".

Making the right decisions

These ethical dilemmas are commonplace and to help us in navigating these, Michael Davis provides a seven-step guide to ethical decision-making that should be adopted by the consultant and the

organization alike:

- 1. State the problem** – what is it about the situation that creates discomfort, presents a conflict of interest or ethical dilemma?
- 2. Check the facts** – what are the root causes of the issue? Do these still hold true and therefore is it still an issue?
- 3. Identify relevant factors** – what are the internal and external contributors to the issue?
- 4. Develop a list of options** – find ways and people that can help solve the issue – the more creative and imaginative the better – as long as it doesn't lead to another ethical dilemma.
- 5. Test the options** – use these tests to ensure the solutions are appropriate:
 - Harm: will this bring less harm than any other option?
 - Publicity: if published in the Sunday Times, will it be okay?
 - Defensibility: would this option be defensible in front of a committee?
 - Reversibility: is this still a good option if the consultant or organization is negatively affected?

- Colleague: what is the response of objective colleagues with this option?
 - Professional: how would this option be seen by the CMI's Ethics committee?
 - Organization: how would NTT DATA's ethics officer and legal counsel react?
- 6. Make a choice** – understanding steps one to five, decide and act on the best route forward.
 - 7. Review steps one to six** – limit the propensity of having to make these decisions again and learn from the process.

I believe certain principles guide the ethics of an organization, and these can be found in its culture. Culture is critical (as immortalized in Peter Drucker's famous adage): an organization can have policies and codes in place, but if the culture is in contradiction to these, they will be futile. It is critical to drive the correct culture from the onset – the recruiting process – and then consistently drive the desired culture from the top down. Leadership can therefore be challenged to choose between revenue and ethics.

Professional consulting regularly faces ethical



“
It is critical to drive the correct culture from the onset – the recruiting process – and then consistently drive the desired culture from the top down. Leadership can therefore be challenged to choose between revenue and ethics.

dilemmas through the type of work it conducts, as well as being at arm’s length from clients. This is why the alignment to a broader set of professional ethical standards, in keeping with a country’s legal framework, is crucial. This is due to the requirement of professional consultants to provide sound advice that will guide organizations through uncertainty. If this advice is not legally or ethically sound, the consultant may be contravening certain legal bounds.

A good example is that of data protection and integrity. As remote work and globalization become more commonplace, professional consultants need to be acutely aware of how data is accessed and transferred across jurisdictions, and whether this is acceptable legally and in line with the client’s policies.

Navigating ethical dilemmas

This is a critical skill set needed for all professional consultants, due to the raft of situations where ethics will be challenged – challenges that become more high-risk and prolific the more senior in the organization the clients are. To deal with these challenges, it is important to always refer to one’s moral compass, which should be closely aligned to

that of the organization.

Dealing with ethical challenges therefore becomes significantly easier if the consultant has the backing of the organization. This behavior must be part of the organizational culture and reputation.

There are a number of ways to navigate ethical dilemmas, including Davis’s seven-step guide as outlined above, but this – as well as any other framework – will fail if the organization does not provide a safe space and culture to call out unethical behavior, or support others when they find themselves facing ethical dilemmas.

I feel that top-down culture, support and forums to keep each other honest are critical. There needs to be a broad-based, conscious adoption by professional consulting organizations to be the guardians of ethics when advising clients, in the same way auditors are intended to be for financial reporting. In his 1987 publication, *In Search of the Moral Manager*, Archie Carroll presents a valuable framework outlining the essential characteristics of moral management (see table).

Immoral management often results from overtly selfish intentions, and not taking the client into account. Although actions may be within the law, they may be designed to find gaps and opportunities

“
There needs to be a broad-based, conscious adoption by professional consulting organizations to be the guardians of ethics when advising clients, in the same way auditors are intended to be for financial reporting.

	Immoral Management	Amoral Management	Moral Management	
Organizational Characteristics	Ethical Norms	Management decisions, actions and behavior are contradictory to what is morally correct. Decisions are not in line with what is ethically expected. Actively negates what is morally implied.	Decisions lie outside that of normal business practices. Management’s activities lie outside the realm of ethics. May imply a lack of moral understanding, awareness or perceptions.	Management actively stands by, and conforms to, ethical standards and practices. Ethical leadership is commonplace for management.
	Motives	Selfish: management is only concerned with personal gain.	Good intentions, however lacks appreciation of the implications on others.	Good intentions: success is desired, but not at the cost of ethical standards.
	Goals	To gain profits, no matter what the cost.	To generate profits. No other externalities are considered.	Profitability within the law and the company’s ethical standards.
	Orientation toward law	The law is a barrier that must be overcome to achieve management’s requirements.	The law stands as an ethical guide and informs us about what we can do legally.	Must abide by the letter and spirit of the law. Prefers to act well above what is required by law.
	Strategy	Exploit opportunities wherever possible. Cut corners when the opportunities arise.	Gives managers free rein if the law is abided by.	Live by ethical standards. Assume leadership when ethical dilemmas arise. Enlightened self-interest.

“

Mental and physical health, moral standards and personal values have taken priority; these areas are therefore clear focuses for organizations who wish to operate more ethically and enhance the experience for staff and clients alike.

to exploit the client's weaknesses and focus on those, and not what is in the clients' best interests.

Amoral management is when a firm needs to develop a product or service, but doesn't have the funding to do so on their own. Rather, they engage with their client, selling the output as proprietary (often for a limited time), on the premise that they pay for the development and tolerate delays that are often inevitable.

Happily, moral management – where the wellbeing of staff and commitments to clients are well balanced – is on the rise. The best way to measure this is to understand whether any party is any worse off than before. As the world has evolved over the past couple of years, mental and physical health, moral standards and personal values have taken priority; these areas are therefore clear focuses for organizations who wish to operate more ethically and enhance the experience for staff and clients alike.

Real value

As organizations and leadership adopt the moral management approach as a standard, the moral compass and ethical standards of the organization and its professional consultants naturally follow suit. This results in significantly greater benefits that go beyond the deal, and reach further into

staff retention, better reputation and ultimately significant growth and financial benefit.

For references, please go to cxomag.com/article/ethics-a-consultants-guide/



Ian Bower is an innovative problem solver with a passion for stretching the boundaries on what is possible and making it happen. He has cross-functional experience through management consulting in Telco media and wealth management, as well as deep industry knowledge within retail banking and wealth management. He simplifies complex problems and technologies into executable strategies and propositions that compliment the overall business needs and direction. His roles have always required an element of lateral thinking and problem solving. He also has experience in digital transformation, agile delivery, customer strategy, innovation, product management, credit risk management and legal recoveries.

CXO
BY NTT DATA



VIDEO

Sustainability Opportunities in the Energy Sector

By Vincenzo Gargiulo, Head of Business Solutions and New Services, Bludigit

Vincenzo Gargiulo, from Italgas Group's digital transformation arm Bludigit, takes us through how the Italian energy giant is supporting the transition to clean energy, as well as their focus on other Sustainable Development Goals – and how this vision and commitment translates to customer attraction and loyalty. With a steadfast purpose, one which has sustainability at its core, the Italgas Group is strengthening its employee engagement and operational excellence too, and building trust amongst all of its stakeholders.

Scan the QR code with your smartphone camera



Elevating Organizational Performance With Design Thinking

By Giselle Chajin Florez, UX and Service Design Lead, Tangity

Overcoming the traditional mindsets that limit the technology landscape requires a refocus on human needs and empathetic design. With learnings from different cultures, the expertise of working within varied environments and the proven results that such creativity delivers, design-led approaches and frameworks are transforming how organizations tackle legacy challenges.

A design-led approach is one that can redefine ecosystem planning and decision-making, helping organizations to achieve lofty goals around digitalization and transformation. This is a view echoed by Forrester in the Design for Confidence in Digital Experiences report that unpacked the importance of simple digital experiences for customers, and the value of design thinking throughout the development value chain with research undertaken by the University of Sydney.

These are just some of the factors currently driving the popularity of design thinking. Companies are increasingly willing to explore its potential and how it can help them to engage with new global markets and harness the creative and expert potential of developers that have operated in a global capacity. However, they need to overcome one key challenge – the traditional mindset that tends to walk hand-in-hand with development and management methodologies.

This is where designers need to step into the conversation, bringing with them the lessons learned from different cultures, the expertise of



working within varied environments and the proven results that such creativity delivers. It is the designer's responsibility to inspire experimental approaches – by showcasing the benefits of design thinking and providing clear steps on how to overcome the challenges that come with such a mindset change, designers can be powerful ambassadors for change.

Overcoming the design challenge

One of the first steps that needs to be taken is to accept that shifts in mindset and approach are not quick or simple. They require foresight, patience and a healthy respect for the organization's need to evolve at the pace that fits. Change, regardless of how beneficial, doesn't happen overnight and some environments are more agile than others.

This agility can be influenced by multiple factors: culture, legacy processes, limited operations functionality, and caution at a time of uncertainty. This doesn't mean that the company can't adopt a new mindset, only that these different dynamics have to be addressed properly – in a way that

ensures every individual, silo and part of the company has the right tools at their disposal.

The question shouldn't be how to remove these differences, but rather how they can influence each phase of development and how designers can adapt their activities and tools to fit within a new culture. This can be looked at from a cultural level in a country – the physical affection of those who live in Italy could be perceived as an invasion of personal space to those who come from other countries, for example – and within the business, building social networks that allow for true connection and interaction. By respecting these differences, designers can open up new pathways to engagement that can take the challenges that may have inhibited design-led approaches and transform them into opportunities.

Facilitating feedback

When undertaking collaborative work, it's not always easy to hear every individual's opinion, especially if the organization's structure is hierarchical. This makes it crucial to think of

“

If you allow for trust to be brokered between different teams and people by facilitating clear communication and feedback, then the doors are opened for better collaboration and freedom of discussion.

alternative ways of gathering feedback from different people at different levels within the company. Their insights and creative thinking processes could be invaluable, but they may be withholding them for fear of crossing a boundary or overstepping their roles.

There are multiple methods that can support this step, but anything from written to anonymised feedback platforms can help build connections and establish more transparent and engaged communication. As research has found, feedback is both an art and a science, making it something that leadership can learn to master to engage more effectively with people and to build stronger workplace relationships.

If a person comes from a place where they think their opinion or way of operating is superior to other people, it's going to cause conflict. However, if you allow for trust to be brokered between different teams and people by facilitating clear communication and feedback, then the doors are opened for better collaboration and freedom of discussion.

Encouraging connections

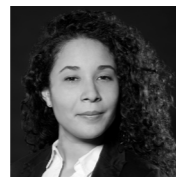
Not all cultures have the same levels of openness or approaches to problem resolution. This can impact trust, collaboration and connections. If participants feel afraid of making mistakes or being judged by others, asking subjective questions or opinions can relieve the tension and encourage people to speak up. It can also allow for people to engage on levels that sit outside traditional business conversations and expectations, which breaks down barriers and

encourages connections.

This is a sentiment reinforced by the PwC Global Culture Survey 2021, which found that there's a direct link between culture and competitive advantage, and that building on different cultures to create a cohesive organizational culture can have a powerful positive influence on talent retention and engagement.

People are the fuel of the business: the creative minds, the inspired ideas. They are the link to design-led approaches throughout the organization. It's their engagement with the company that will see it shift from legacy mindsets towards more open, engaged and collaborative experiences. And the foundation for this shift is trust. Focus on building this trust by allowing for people to communicate freely and giving them the platforms and spaces they need to thrive.

For references, please go to cxomag.com/article/elevating-organizational-performance-with-design-thinking/



Giselle has worked in Service Design at Tangity for seven years. In 2018, she led the first NTT DATA design studio in Tokyo, applying various service design methodologies and supporting colleagues in setting up new projects. There, she led projects in both the public and private sectors, putting her in touch with the authentic Japanese work culture while understanding differences between the Eastern and Western worlds. Giselle has led projects in Germany, Australia, US and Japan.

5 Minutes On...

Authentic Leadership

By Nick Craig
President of Authentic Leadership Institute and author of *Leading from Purpose*



Nick gives CXO 5 minutes on starting the Authentic Leadership Movement, how to truly be yourself, and how purpose helps leaders find solid ground in a VUCA environment.

Scan the QR code with your smartphone camera



How Customer Empathy Drives a Successful Omnichannel Strategy

By Daniele D'Aquino, Senior Engagement Manager, NTT DATA Italia

If the past two years have taught organizations anything, it's that empathy is an essential part of customer service and engagement. This is the right time for organizations to focus on building a culture of empathy by developing processes that promote empathetic customer experiences and engagements through tailored interactions and smart technology.

“

Customer empathy builds trust and loyalty which, in turn, lead to improved experiences as customer service connects on a more human level.

In the gap between a customer's actual experience and the one intended or promised by a brand, lies the potential for frustration, anger and diminished loyalty. It is here that customers make the decision to leave, and where a brand's reputation can falter. This gap has also widened over the past two years due to the limitations imposed by the pandemic – communication became digital, channels were put under pressure, customers felt isolated and service was largely reactive thanks to limited customer touchpoints and engagements.

In 2020, Gartner emphasized the importance of a proactive customer service roadmap that focused on, among other key elements, the development of human resources that have the skills required to engage with customers more in-depth. In 2022, this conversation evolved with Gartner underscoring the importance of focusing on both customers and employees to drive growth: a growth enhanced by customer-centric processes that put empathy and trust at the forefront of engagements.

With improved customer experiences voted as the leading indicator of strategic performance in the Global Benchmarking Report from our sister company, Dimension Data, for the eighth year in a row, recognizing the person behind the engagement has never been more important. Customer empathy builds trust and loyalty which, in turn, lead to

improved experiences as customer service connects on a more human level. It's easy to see why companies should be paying attention.

Empathy, trust and loyalty

The scale of empathy is directly connected to the scale of trust that the organization needs to foster to increase loyalty. Research has found that brands that connect effectively with customers are those that 'engage, entice and enrich'. Empathy and trust are intricately connected, a consequence of one another.

Empathy is not just the connection made between the agent in the call center with the frustrated customer sent from pillar to post, but the connection between organizations that work with one another to provide and consume services. By creating an environment that fosters empathy within the business, the organization is creating a space within which this behavior will flourish.

One of the prerequisites for building this empathy is to have access to customer insights. Customer data is essential to understanding and predicting customer needs, motivations, behaviors and intentions. With this picture painted by data, contact center agents can see how customers respond, what their pain points are and how to react to these in ways that will engender positive interactions – and

“

Data is essential to understanding and predicting customer needs, motivations, behaviors and intentions. With this picture painted by data, contact center agents can see how to react in ways that will engender positive interactions – and build trust.

build trust. If agents have all the information about the customer, they can leverage this to personalize experiences.

Insights from this data can also be leveraged to build and strengthen further customer connections. Voice of the Customer (VoC) is the roadmap to empathic engagements that fully understand customer feelings, while using a variety of different tools: direct engagements (surveys), indirect engagements (social listening, speech and text analytics), and inferred engagements (behavior and transactional analysis). All this data can be gathered to help better know the customer and connect with empathy.

Supporting a successful omnichannel strategy

The vast volumes of data collated from across the omnichannel journey plays a significant role in helping the organization to understand customer needs. It helps agents to unpack whether or not an interaction requires a high level of empathy, or if the customer would be better served using a self-service channel. This is an important consideration, because while digital channels can run 24x7, they need to be balanced with human interactions (in order to provide the connection and support that people really need).

To foster this empathy throughout the omnichannel strategy and the business, companies need to create genuine connections through routing logics that match the customers with agents that will more likely get along with them and make them feel understood. This is no small thing – one person's superb contact center agent may be another person's disconnect.

Usually, routing logics consider agent skills as technical expertise, ability to retain customers or to sell services and products. Empathy should be a skill to take into consideration as well, especially with customers who show an emotional condition that needs a higher level of empathy (i.e. angry, complaining customers). Pairings could also consider other elements, such as the same geographical location, or shared hobbies. These can foster connections that go beyond just a problem, a call and a resolution.

Another way of building strong connections is to use video. Most people have become accustomed to using it over the past two years so it offers them the ability to engage with someone face to face – something that can minimize conflict in itself – and reduces a sense of isolation and distance.

For companies that want to add even more heft to their empathic engagement roster, there is now the option to add in chatbots that have empathy built

“

An empathic chatbot can fill the gaps in customer communication and help organizations build a richer customer connection. Empathetic or emotional AI can mirror customer emotions and knows when it's time to hand a person over to a human agent.

in. These virtual assistants are often considered the least empathic of all digital touchpoints, but the next generation can process and react to human emotions. As research has found, an empathic chatbot can fill the gaps in customer communication and help organizations build a richer customer connection. Empathetic or emotional AI can mirror customer emotions and knows when it's time to hand a person over to a human agent if they need richer engagement or support.

A more connected future

Recent years have seen an increased need for empathy in customer service. Organizations must strive to establish a culture and processes that facilitate a more empathetic customer experience, making full use of technologies to anticipate customers' needs and offer a tailored experience.

It's not easy to transform the empathetic register of an entire organization, but iterative changes in technology, training, culture and omnichannel engagements will deliver results. While there's no magic bullet, with a commitment to shifting legacy approaches towards a way of doing business that's open, informed by data, and driven by trust and empathy, companies can build meaningful connections with customers – and in turn create revenue-driving loyalty.

For references, please go to cxomag.com/article/how-customer-empathy-drives-a-successful-omnichannel-strategy/



Daniele D'Aquino has over 15 years' experience in Customer Services and the Telco/Media industry. Since 2016 he has been in the Customer Operations (R)evolution focal point in NTT DATA Consulting, a role that has given him the opportunity to work on several key projects and coordinate a variety of commercial propositions related to CRM and Contact Center. Daniele is enthusiastic about new technologies and the impact they have on business models and customer behavior.

5 Minutes On...

Engagement Strategies to Attract and Retain the Right Talent

By Ric Garner
 Managing Director, Future of Work Consulting Practice, NTT DATA Services



Ric gives CXO 5 minutes on how to optimize employee experience from the very beginning to win and develop talent, how generational differences affect engagement, and how leaders can accelerate and support workplace transformation.

Scan the QR code with your smartphone camera



Technology, Ethics and Customer Trust

By Vincenzo Iucci, Director, Security, NTT DATA Italia

Companies that want to differentiate themselves will have to take a long, hard look at their practices around safeguarding customer data. Practices need to comply with the relevant laws, of course, but they also need to be rooted in ethics. Risk governance technologies make it easier than ever before for companies to be both compliant and ethical – and prove to customers they can be trusted.

In the beginning was the business, and the business was with data, and the business was data... Whether your company is large or small, personal data is the foundation of trade – helping to derive customer insights, drive personalized services and make accurate market predictions.

Then came the law: regulations stated that personal data is owned by the people who generate it, and not company property; that those collecting data have to give users full control of how it is treated, and carefully safeguard personal information.

The natural human reaction to a new rule is to find the quickest way to appear compliant by modifying one's behavior as little as possible – even if doing so ignores the spirit of the legislation. This is generally possible, because the law has shades of gray. Ethics, however, can be seen as binary – decisions and behaviors either align to your values, or they don't.

Business ethics are a relatively recent phenomenon, having for many years been viewed as superfluous. But business is a matter of trust, and

today people are more aware of how their data is collected, used and turned into money. They are also informed daily about breaches and worried about a sense of 'surveillance' that undermines their privacy.

Trends show how people don't trust that organizations will keep their data safe, nor that they will collect clear consent. There are also fears that organizations will sell data without permission, or store more data than necessary. It is precisely this growing lack of customer trust in organizations that is transforming the perception of ethics from a cost to a market differentiator.

In this complex scenario, current and emerging technologies are key in making sustainable, ethics-driven choices.

Be crystal clear from the beginning

To cultivate the trust of customers sharing their data with companies, it is necessary to be clear from the outset. The more consciously data is shared, the greater value it brings to those collecting it. The law requires that companies explain in simple, concise

terms what they intend to do with data, to whom it is eventually transferred, why, and in what form.

Beyond that, blockchain technology could be used for consent management to ensure consent is continuously tracked, and that every subject can revoke consent if they wish. Blockchain could also be used to provide visibility to data subjects of every instance of access, transfer, transformation and deletion of their data, both at the level of a single organization and potentially also at the level of aggregate systems such as a market sector, or even a country.

Be fully aware of what you've got

Personal data that organizations collect is usually the result of several campaigns executed over time. The regulatory framework evolves. The social environment changes. Organizations merge with each other or transfer branches to other companies. Top management revamps the business model to align with or anticipate the market.

Therefore, often companies don't have full knowledge of the personal data they manage, or



“

It is precisely this growing lack of customer trust in organizations that is transforming the perception of ethics from a cost to a market differentiator.

this knowledge is spread over many operational functions without an integrated overview. Technologies in the data risk governance domain make it possible to maintain an up-to-date, comprehensive and detailed view of all the personal data processed by an organization, as well as determining the exact distribution of the relevant data for each individual.

This enables the execution of subjects' rights and supports the risk management process, but is also a deeply ethical choice in itself, because it generates awareness and a sense of responsibility, and enables cascading others' choices.

Keep only what you need

Much of the data that companies collect is not used for either contractual or statistical purposes – but because it might be useful someday.

Instead, the ethics-driven choice is to collect only what is needed and eliminate what is not. This serves the privacy of the data subject, decreases the impact of a possible data breach and makes the business more environmentally sustainable by decreasing its carbon footprint.

Move value, not data

To maximize value, data is often moved around and shared with third parties. This widely

increases data-related risks, sets specific needs in terms of consent management and may reduce customers' trust.

Today, however, it is possible to acquire insights from data without accessing or transferring the data itself, such as via an Internet of Trusted Data (offering both auditable verification of identity and data credibility), as well as homomorphic encryption (making it possible to analyze encrypted data without revealing it).

Using these new technologies, data is kept safer in fewer places, and the algorithms only exchange non-identifying statistics. Therefore, corporate functions can ethically work together to facilitate the flow of insights, with the common goal of acquiring maximum value from the data.

Apply deletion with no fear

Privacy regulations require that data is deleted if explicitly requested by the customer or after a given period. In complex business ecosystems, the deletion process can be onerous and challenging, given the extreme fragmentation of data that, in many cases, exists among business applications.

Again, the detailed knowledge of data distribution provided by data risk governance plays a key role here: full data observability can provide the tools to set an effective retention policy

“

Truly embracing the defense-in-depth approach can demonstrate to customers that an organization is treating their personal data as carefully as they would.

and help business functions to be fully aware of the risks of non-deletion.

Protect data in depth

In most cases, data protection is done through technology that provides access control. The concept is absolutely valid, but in a time when the risk of data exfiltration increases daily, it's necessary to identify supplementary security measures. Technologies such as Information Rights Management (IRM) or Attribute-Based Encryption (ABE), for instance, greatly enhance data security by protecting not only the container, but also the content.

Reviewing data protection policies by considering risks holistically, and truly embracing the defense-in-depth approach (the use of coordinated, multi-layered security measures), can demonstrate to customers that an organization is treating their personal data as carefully as they would.

Embrace ethics to keep market share

The fact that many global technology companies are putting the care of customers' personal data at the center of their business is no accident. Privacy ethics is a reality, and its implication in terms of increased consumer trust is already visible. Ultimately, it's no longer a nice-to-have: almost all

players across many market sectors must embrace ethics – or lose market share.

There is an expanding tangle of growing business needs, more stringent privacy regulations and higher standards of ethics. Luckily, technology can help us unravel it – providing better outcomes and higher trust not just for customers, but for the organization itself.

For references, please go to cxomag.com/article/technology-ethics-and-customer-trust/



Vincenzo Iucci discovered a passion for cybersecurity during an internship and made it the common thread of his career path. In NTT DATA since 2007, he has been involved in many technologies in the cyber field. Since 2018, he has been responsible for the Information & Data Protection practice.

The Value of Trust in Business Relationships

By Claudia Jandl, Head of Industry Consulting, NTT DATA DACH

Today the global operating environment stands on shaky foundations. Technology is changing at unprecedented rates, and with significant political and economic instability, uncertainty defines interaction, experience and strategy. To build a future that can withstand this complexity, organizations need to put trust at the forefront of their engagements and operations.

“

The role that brand perceptions play in establishing trust should not be underestimated.

Trust has never been harder to earn or easier to lose than it is today. As much a commodity as the services that an organization provides, trust is the foundation on which the organization should be building its future. It's a culture of trust that ensures employees remain focused, productive and committed; and it is trust that must become the organization's most important metric of success. Brands operate as an identifier for the customer and are associated with a certain level of quality, risk, and value. If a brand's perceptions are positive, this creates trust that resonates throughout engagements between customer and company.

This is particularly relevant when it comes to business-to-business (B2B) engagements within the services industry. Unlike tangible products that have weight, taste and sensation, services are harder to quantify. This makes it essential for any service-based organization to build relationships with customers based on reliability and trust.

A few years ago whilst writing a paper on brand building in the B2B industry, I investigated the value of trust. The most important areas for organizations to focus proved to be: risk reduction, social visibility, competitive differentiation, service complexity

reduction and value for money. By prioritizing these areas, organizations can strengthen not just their relationships but their reputation.

Relationships and reputation

Customers need to trust in the information they receive from service providers in order to feel they are getting a fair exchange of value.

Based on my research on trust which found that reducing perceived risk is a key driver for selecting a partner in the services industry, the question that every service-based organization should be asking is: what can we do to ensure the information and services we deliver are perceived in the right way by our customers?

One of the most important metrics of trust today is an organization's image: the role that brand perceptions play in establishing trust should not be underestimated. This is particularly relevant in the consulting industry where the services provided are complex, and where technology implementations run the risk of failure or limited return on investment. But when an organization is trusted, customers believe in its ability to manage complexity.

Another increasingly important element of today's

“

From my perspective, the companies that embed trust into every aspect of customer engagement – through honesty, transparency and collaboration – will lead the way.

business relationships is social visibility. Companies that have an established reputation and a proven track record, along with ethical and environmental commitments, are going to start this journey on the right foot, and several feet ahead of the competition. In practice, this means the first steps any company should be taking are to:

- Clearly define policies around environmental, social and governance (ESG) issues;
- Embed transparency into engagements across company and customer;
- Ensure equally well-defined policies around business practices and ethics.

In a recent analysis of ESG and its implications for brands and perceptions, the McKinsey Global Survey found that companies getting significant value from their sustainability programs are those that follow certain types of management practices: those that are more inclined towards transparency, value creation and customer engagement.

So, I believe that to ensure services are perceived in the right way by customers, businesses must commit to ethical and transparent processes – shaping a company that's trustworthy across every layer, employee and engagement.

Trust-building actions

What is required to really shape trust? Brand ethics and a commitment to ESG play a significant role, but there are additional steps the organization can take to really embed this trust.

Agile working models are key, allowing for organizations to engage in partnerships more effectively, building on a foundation of collaboration that puts the customer's business at the center of decision-making. This allows for the relationship between the service provider and the customer to evolve intelligently – to deftly shift service provision and approaches to meet the changing needs of the customer's business. Most companies have a vision of this level of collaboration, but many have no clear roadmap.

In the past, targets were clear and roadmaps were easily defined based on business plans and waterfall charts. But this is not the case today, in a constantly shifting landscape. The future is hazy and complex. This makes trust incredibly relevant right now – customers have to trust in what the company delivers. They have to trust that companies mean it when they say 'we're all in the same boat'.

Companies that recognize the value of this,

“

Failure happens. But with the right partner, it should not define the end of trust. Instead, failure should become a benchmark for improvement and transformation.

that share in the wins and the failures, are the gamechangers. From my perspective, the companies that embed trust into every aspect of customer engagement – through honesty, transparency and collaboration – will lead the way.

I believe that organizations need to take a more holistic approach to trustworthiness. That they focus not just on perception, but on sustainability and ESG commitments, on employee wellbeing, and retaining its relevance in a competitive and innovative space.

The trust connection

At NTT DATA, we strive to become a service partner, rather than a service provider, for our customers – providing consulting services and engagements that focus on collaboration and sustainability. This goes beyond just the promise made to the customer, but how internal employee values are aligned with the ideals of trust, innovation and shared responsibility.

Within the service industry, built on the shoulders of employees and smart people, failure happens. But with the right partner, it should not define the end of trust. Instead, failure should become a benchmark for improvement and transformation. Having clearly defined metrics around managing

failure, transformation approaches, and ensuring transparency is the basis.

While trust initially seems a relatively hard-to-grasp criteria for business success, companies can take very clear actions in their target operating model. Trust then becomes inherent. It comes as standard: as much a part of the service delivery as the technology.

For references, please go to cxomag.com/article/the-value-of-trust-in-business-relationships/



Claudia Jandl heads the industry consulting practice at NTT DATA DACH. With her team she provides consulting and solutions to her clients in various industries supporting their digital transformation journeys. Before joining NTT DATA, she worked nearly ten years for an international consulting and market research firm in various positions. As part of her Executive MBA in 2013 she researched the importance of brand building and trust for service providers.

VIDEO

Trust: The New Imperative for a License to Operate

A film by NTT DATA

Trust matters more than ever, but in the age of (mis)information, knowing who and what to trust is becoming increasingly difficult. The challenge to prove good corporate behavior is matched by the opportunity: trustworthy businesses have a competitive advantage extending from talent and customer attraction to organizational excellence and stronger growth. Forward-thinking leaders understand that trust is an economic asset, and a crucial one. As consumers and employees alike pay more and more attention to the business practices and social impact of brands, only those that demonstrate authenticity and social responsibility will have a license to operate.

Scan the QR code with your smartphone camera



Lessons From the Past to Guide the Future: Humanity in Cybersecurity

By Ortwin Maier, Head of Cybersecurity, NTT DATA Romania

Creating effective cybersecurity systems is about so much more than understanding your vulnerabilities and putting measures in place to mitigate them. It begins with understanding what has made human beings feel safe in the past, and using those lessons and behaviors to build an electronic world they can trust.

When I was a boy of just five or six, each evening at dusk I would run out of our yard, into the streets of our small village, and wait. I was waiting to see the lantern of the night watchman as he moved through the village. His job was to ensure that each villager woke in the morning with the same number of animals they'd had the night before. His job was to create a sense of security and trust.

In a sense, that was a microcosm of what we're looking for when we contemplate cybersecurity in our hyper-connected world: creating security and trust for organizations on the one hand, and for our employees and customers on the other.

If you're not taking cybersecurity seriously, you should be asking yourself why. Cybersecurity dangers are the biggest concern for companies globally in 2022, according to the Allianz Risk Barometer, and Cybersecurity Ventures predicts that global cybercrime costs will reach \$10.5 trillion annually by 2025. Creating trust, security and accountability in the electronic world is our most pressing challenge.

So how do we do this effectively? The answer, I

believe, is twofold: we need to look backwards, using the past as a benchmark; and we need to plan with real foresight, understanding the true scale and nature of the problem.

Looking to the past to guide our thinking

If we think about information exchange historically, hundreds of years ago people communicated via a paper roll with a wax seal, so that the recipient could be certain their message had not been tampered with. More recently, we placed letters in envelopes that we glued closed for the same reason. There were rules in the legislative framework of society governing how you treated those communications, rules you had to obey, that safeguarded privacy and created trust.

We also built castles around ourselves – or walls around cities – because we understood that we could not protect ourselves adequately alone. And then we added a moat to make an attack even more difficult. Both individuals and society at large understood how those fortifications worked – they

could see them for themselves. They could assess exactly how thick and high the walls were; however deep the moat, they could understand it.

The challenge in the world of cybersecurity is that the individual lacks this understanding. It's a completely new aspect of society that they haven't been trained in for thousands of years. Most individuals barely have a basic understanding of cybersecurity – because most of this knowledge resides in the domain of corporations.

Trust and the individual

To bring individuals into the cybersecurity fold, we need to understand how trust functions in their minds, and use the behaviors that are already embedded deeply inside them. The archaic patterns of trust and security still work, but the electronic world adds an extra layer. We need to find a way to create a culture of trust covering this additional layer, and generate acceptance within people's thinking.

We have tried to build electronic trust within institutions by validating user and device identity



“

Employees work in small, interconnected satellites – connected with the company, each other, and the world at large – and we need to build small spheres of security around each one.

at the system point of entry, identifying and mitigating against vulnerabilities – and by doing everything possible to ensure our infrastructure is both threat-resistant and risk-tolerant. However, we haven't truly understood what gives individuals a feeling of safety.

We've moved swiftly from mainframes to networks and a more disseminated model of computer work, to the ultimate network – the internet. Using the internet has become fundamental; to participate in the electronic world you need to use it. And if everyone needs to use it, then talking about trust and accountability means we need to think globally.

We also need to realize that the Covid-19 pandemic pushed us into the next stage, which is not a disseminated model so much as an atomized one. It's not even about working from home: employees can work from anywhere now. No longer do 2,000 people arrive at work at the same time and leave at the same time – the shift has happened, and there's no indication that the working world will return to its former model.

Now employees work in small, interconnected satellites – connected with the company, each other, and the world at large – and we need to build small

spheres of security around each one. The same applies to consumers, who interact very differently with companies now.

For instance, consumers interact with companies far more on digital channels now, particularly in the aftermath of the pandemic, and as a result are taking more control over how their data is used and secured. They, too, need spheres of security around them – which means we need to find solutions to cover the entire chain of reliability.

Planning for the future

The challenge is to bring the security of those satellites to the same level as that of the corporation. As we do that, we cannot afford to neglect the human aspect, because trust is partly a logical proposition, and partly an emotional one – we put our trust in other human beings, whether or not that decision seems rational.

This means that those of us who work in cybersecurity will need to be well skilled in communication – and not many of us are. Basic communication skills are not taught in schools and universities, so we will need to build that expertise, and educate ourselves in being human.

If we don't invest in learning to communicate

“

Trust is partly a logical proposition, and partly an emotional one. This means that those of us who work in cybersecurity will need to be well skilled in communication.

well, employees will not have any empathetic relationship with the companies they work for, and those companies will become interchangeable. How we are joined together depends on the emotional domain – we can't treat people like robots. What we need instead is to create awareness about cybersecurity concerns and take action, and start talking about them in a new way, in a human way, with understanding. And we need to do all of this in the so-called post-truth world, where the manipulation of truth and creating uncertainty have become industrialized.

In this environment, then, how do we seal the scroll, glue the envelope closed, light the watchman's lamp? We watch and guard the process, and allow for legal frameworks that can govern the virtual world. We thoroughly educate individuals about the dangers they face, and take the threats seriously ourselves.

And we plan for a future where we build trust in all of our institutions with an understanding of human behavior, with empathy, and above all, with true foresight – the kind of awareness and planning that will enable us to respond quickly and effectively to future threats.

For references, please go to cxomag.com/article/lessons-from-the-past-to-guide-the-future-humanity-in-cybersecurity/



Ortwin Maier's vibrant career path encompasses leadership positions across the Intercompany and Emerging Market businesses, as well as Delivery Assurance. He is also a seasoned business developer and IT entrepreneur. Driven by his passion for technology and growth, his extensive experience positions him today as the Head of Cybersecurity.

Future Fit: Implementing Cloud-Based ERP the Right Way

By Ulrich Kreitz, Head of Managed Services Germany, NTT DATA Business Solutions

Enterprise Resource Planning is a key piece of the puzzle when it comes to turning operational excellence into competitive advantage. But as the cloud opens up opportunities, relationships between clients, services and suppliers are changing. As suppliers are being asked to accept more client risk, and own processes in the future, success in the new world will come from carefully building trust.

From integrated information and streamlined processes to cross-department collaboration and accurate forecasting, Enterprise Resource Planning (ERP) offers many competitive advantages.

Much has been written on the subject of the future of cloud and ERP environments from a high-level perspective (with reports of the global ERP market reaching more than \$66bn by 2026), but my focus, in this article and throughout my career, is on the real-world implementation. Strong relationships built with clients have always come through improving processes and delivering tangible results.

It is from this perspective that I have viewed recent changes in the delivery of ERP products. Naturally, this has given me a useful starting point to look to the future too. As more cloud-based technology comes online and opens more exciting opportunities for optimization, product offerings across the sector are evolving. The most important thing for me is that the way we work with our clients ought to be developing in parallel. The sense of partnership and need for trust is growing, as roles, responsibilities and boundaries shift.



How should organizations move forward, to ensure that the personal connections within client engagement are nurtured, in conjunction with embracing new tools and ways of working? And what are the implications of today's changing landscape? Here, the cloud, new business models, new customer requirements and shifting roles and responsibilities all come into play.

The impact of the cloud

At NTT DATA we have spent the last few years demonstrating how the cloud, and all its benefits, is revolutionizing client ERP landscapes. We are clearly not alone in understanding its potential: the cloud-based ERP software market is expected to grow by 13.6% annually. Furthermore, 50% of existing ERP customers said they would explore new suppliers to renovate or replace their systems.

Of course, each customer has unique goals. We recently helped a discrete manufacturing client replace a heterogeneous landscape with one central system of standard delivery processes, across their global business. But change might

mean starting small with a pilot piece of work. Our manufacturing client started with one location, for example, delivered in an initial six-month period, before moving on to implementation across 24 countries. Supplying vital air and water filtration equipment globally, it was important supply chains remained uninterrupted as they were modernized. Testing becomes important when, as is sometimes the case, a business commits to a cloud-based ERP product without fully understanding the impact of implementation in detail.

Delivering any solution also often means negotiating with software partners who, of course, have their own vision and strategy. Data handling is another consideration. The customer's own, suppliers' or third-party hyper-scale data storage centers are all options to review.

New business models

Given the variables and complexities at work, implementing, integrating and managing today's ERP solutions have led to new ways of packaging and selling solutions. The direction of travel is away

“

Being able to offer easily-integrated additional products alongside core cloud industry solutions will add value – solving more of their problems. What better way is there to position yourself as a go-to trusted partner?

from selling software licenses, hosting, maintenance and managed service packages and towards a more consultative model. This means subscription pricing replacing more traditional models based on user numbers and software updates and renewals.

We have seen that contract lengths are increasing from one, to three, to five years. One immediate impact of this shift is the loss of cash flow associated with an initial upfront software investment. For customers to become profitable for us in the future, we will need to work harder to grow value over whole contract periods. Forming strong relationships and providing quality support will only grow in importance.

Further development of independent Intellectual Property (IP) is also likely to become an increasing part of making money from customer relationships. Being able to offer easily-integrated additional products alongside core cloud industry solutions will add value. Extending what is offered to customers means solving more of their problems. What better way is there to position yourself as a go-to trusted partner?

New customer requirements

Customers are changing too. As time goes on, more

will turn away from wholly bespoke systems.

Efficiently adopting cloud-based ERP might mean accepting more off-the-shelf processes and adopting existing best integration practices. Examples include delivery through preconfigured mobile apps and integration via standard whitelisted APIs.

Others will, perhaps, struggle with the idea that getting the best results from the cloud might mean finding new ways to work. For many, there are operational and market obstacles to overcome too. Covid-19 and other socio-political uncertainties of the last two years linger. Given these circumstances, it is likely many companies won't have much spare energy to invest in their ERP rollout.

Shifting risks, roles and responsibilities

Therefore, suppliers like us are being asked to accept more of the client risk, and own processes in the future. Being a trusted supplier means taking accountability when things don't run smoothly too, because clients' resource availability is increasingly stretched. There is still a lot of work to do for suppliers here. As recently as 2019, 45% of ERP projects suffered cost overruns and 58% were not delivered on time, according to a report from Panorama Consulting.

“

Today's landscape sees a clear opportunity to seize the initiative, understand the product benefits, build services that create genuine value and, most importantly, continue to deliver real, lasting positive operational results.

Today ERP implementers, such as NTT DATA, feel in a state of flux. Can we keep customers' trust through this period of evolution as we adopt, and adapt to, new cloud-based solutions?

I am confident the answer is yes. If you are in the business of using or implementing cloud-based ERP systems, today's landscape sees a clear opportunity to seize the initiative, understand the product benefits, build services that create genuine value and, most importantly, continue to deliver real, lasting positive operational results. However, both suppliers and customers will have to be flexible as change gathers pace. Achieving this won't happen overnight. It will need care, thought and confident leadership.

We are all going to have to look at our supplier offering. Longer, more consultative contracts are likely. We will have to share more risk, too, as we deliver more responsive and innovative products. So, trust me when I say it is an exciting time to be in our industry.



Ulrich Kreitz has been an SAP Consultant for more than 15 years and since 2011 has led the NTT DATA Business Solutions process consulting team. One of his focal points is complex ERP implementation projects in large enterprises. His projects have been awarded with the SAP Quality Award Gold and the NTT DATA SE Grand Award. Since 2017, Ulrich has overseen the ERP Cloud business, covering products such as SAP S/4HANA Cloud and SAP Business ByDesign.

For references, please go to cxomag.com/article/future-fit-implementing-cloud-based-erp/

Cybersecurity is Everyone's Job

By Alexis Martín García, Cybersecurity Analyst, NTT DATA EMEAL & Marcos Búrdalo Romero, Cybersecurity Analyst, NTT DATA EMEAL

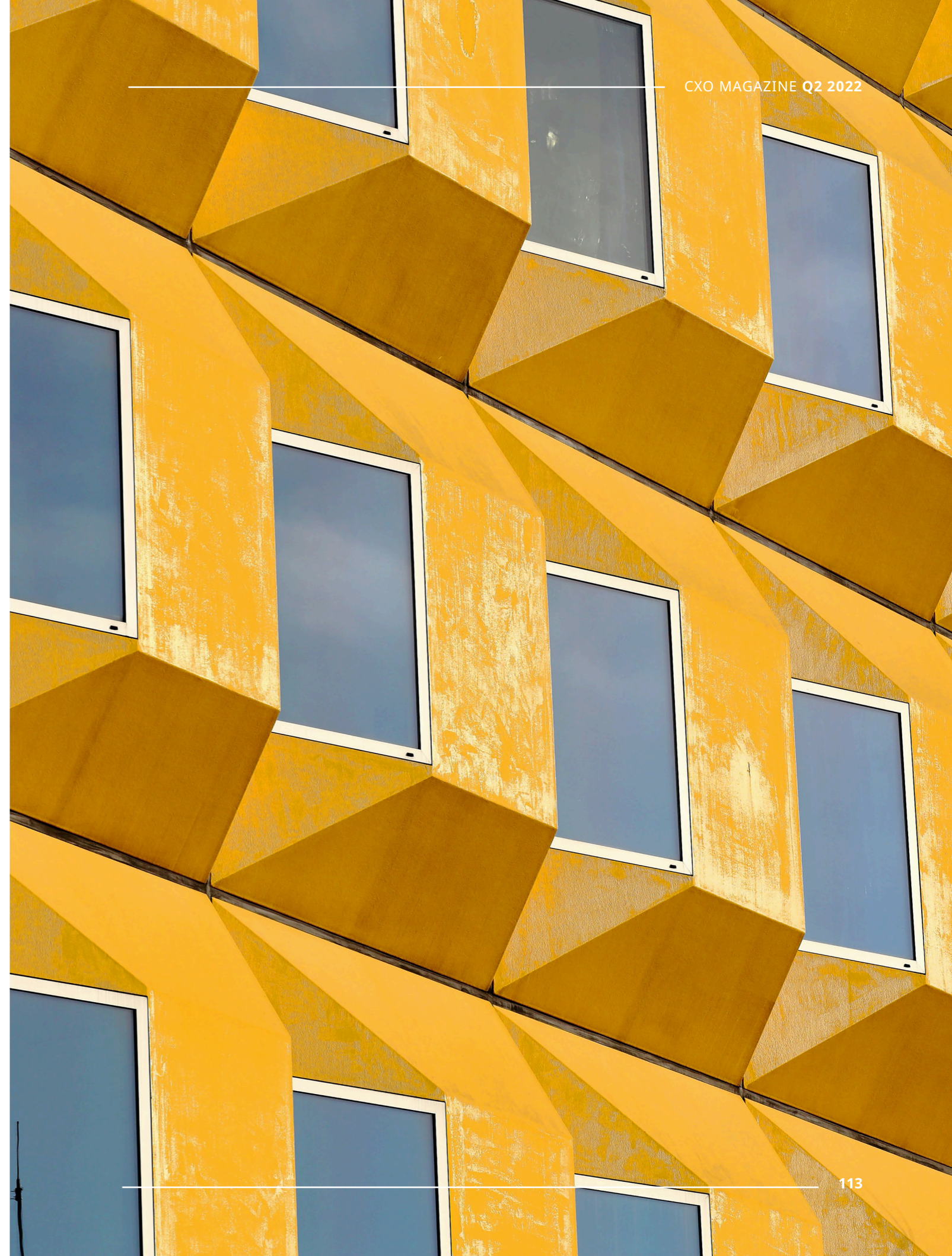
In a hyperconnected world, cybersecurity is a vital part of protecting both corporate reputation and the safety of employees. While IT departments might be responsible for putting systems in place, it takes every employee from the C-suite down to ensure those systems remain intact.

When asked what assets a business holds, most would think of buildings, land and cash. But there's a less tangible yet nonetheless highly valuable asset that many forget: reputation. Difficult to acquire and easy to lose, brand reputation is vital in allowing a business to succeed, irrespective of how good its services or how efficient its infrastructure.

The bedrock of brand reputation is trust – without it, reputation cannot exist. And one of the key ways to build this trust into a business today is by developing a multi-faceted cybersecurity strategy – one that takes the full gamut of threats into consideration.

As far back as 2017, digital security company Gemalto (since acquired by Thales), identified in a survey that 70% of consumers would stop doing business with a company if it experienced a data breach. In addition, PwC's 25th Annual Global CEO Survey found that CEOs rank cyber risks as the top threat to growth. Yet many companies still fail to take cybersecurity seriously until there has been an incident – at which point it is already too late.

There are also financial considerations:



“

Attackers might set up fake websites or emails in your company's name, which might well be indistinguishable from the real thing to the ordinary person.

companies that fall prey to cyber attacks can lose money to ransom payments, unapproved money transfers, a negative impact on their share price, the cost of investigating the attack, and in repairing the damage. In addition, there may be legal costs for not taking proper care of customer data. Your cybersecurity defenses, therefore, need to be as stringent and comprehensive as possible.

Getting employees on board

First, be aware that the way employees use company networks and systems can unwittingly pose an enormous risk to your cybersecurity. Here, passwords are a major problem – if they decide to use the same password to access their personal and corporate social media accounts, for instance, that could expose you to risk – if you have a data leak, cybercriminals could access your corporate emails and compromise you.

It's important, therefore, to educate employees on the importance of strong passwords, and have a clear password policy in place. Passwords also need to be renewed regularly so that if they are compromised, the window of opportunity for any breach is very limited.

Overlaying this should be two-factor authentication; that way, if one level of authentication is compromised, the next one will block any unwanted access.

Beyond passwords

But while good password control is vital, there are many other risks to consider – and more are emerging every day. This requires that your in-house cybersecurity team conducts continuous monitoring to keep the system as updated and secure as possible as new threats appear – and anticipate any leaks or weaknesses that cybercriminals might exploit.

Phishing and impersonation attacks, for instance, can cause a great deal of damage, where illegal access is gained to bank accounts, or an attacker poses as a trusted person (or company) to steal money or sensitive data from a company. Attackers might set up fake websites or emails in your company's name to achieve this, which might well be indistinguishable from the real thing to the ordinary person.

Hactivism, too, poses a serious risk: hactivists gain unauthorized access to company or government files or networks to further their own social or political goals, and can cause enormous reputational damage if those views are seen as being aligned with your organization.

And then there is the use of ransomware, where a company's data is stolen, and a payment is required. Ransomware attacks in 2021 cost companies in a variety of industries millions of dollars, and the damages aside from the ransoms

“

Constantly test the system – and ensure defenses are in place for data going in and out of the company, as there are risks in both directions.

averaged \$4.62 million, with mega-breaches costing as much as 100 times more.

Prevention is better than cure

Of course, there are no guarantees when securing your company's networks and data, but there are a few vital pillars to ensure they are as secure as they can be. Having the right measures in place can give your organization a fighting chance when attackers attempt to breach your defenses.

First, ongoing education of employees is vital. They must understand how phishing works, how their passwords help to keep the organization safe, and how to identify suspicious emails, links and websites. Most of all, they must learn to be vigilant at all times, and additional training must be given as and when new threats arise.

Second, it is important for your cybersecurity team to constantly test the system, and ensure defenses are in place for data going in and out of the company, as there are risks in both directions.

And third, it's imperative to understand that this is not a one-off intervention: cybersecurity must be monitored and updated around the clock, on a continuous basis, and that requires a specialized team, and support for the necessary interventions from the company's executive management. Without that top-down support, it is very difficult to get the rest of the organization on board.

Getting everyone on board is a key strategy, because good cybersecurity is a team effort – not just from those working in the security department, but from every person in the company. It's a new way of working for many and will take some adjustment. But if everyone works together, it is possible to build a system with strong resilience against potential attacks, and most importantly, a system that does its essential part to keep the company's reputation intact.

For references, please go to cxomag.com/article/cybersecurity-is-everyones-job



Alexis Martín García is a Cybersecurity Analyst and leads the NTT DATA EMEAL Hacking Security Office team. He has performed tasks such as web, mobile, infrastructure, Wi-Fi security audits, red team exercises and social engineering

awareness campaigns in addition to collaborating with the management of the Cybersurveillance team in Spain.



Marcos Búrdalo Romero is a Cybersecurity Analyst of the Hacking Security Office team of NTT DATA EMEAL. He has performed tasks such as code, infrastructure, mobile and web security audits, red team exercises or social engineering awareness campaigns.

Trust or Bust – Why Transparency Matters

By Lisa Woodley, General Manager – Northeast, Nexient, an NTT DATA Company

In a post-pandemic world of rising prices, broken supply chains and disruptive technologies, where do trust and transparency fit? Are they nice-to-have luxuries or essential components of success? If they are essential to success, how can businesses deliver them to increasingly cynical consumers?

Every so often there comes a turning point when something happens that changes people's thinking in a big way. Sometimes it's triggered by a political event, a pandemic or a war. But in the middle of March 2018, it was a newspaper story about a little-known British political consultancy called Cambridge Analytica being given access to what would amount to 87 million Facebook accounts without their users' permission.

Until then, media stories were about data breaches, a matter of cybersecurity. This took us into a whole new, emotionally charged territory of data abuse. And that was a matter of business ethics and corporate morality. There was a realization that the information we were giving others wasn't being used in our interests but theirs, and we were angry about it. Suddenly, the whole issue of trust was in play.

Four years on, trust – or rather lack of it – has become an even more toxic issue thanks to an endemic failure of leadership, both corporate and political. Take a look at the 2022 Edelman Trust Barometer and you'll see that distrust is now the

default position for many. Then read the Adobe Trust Report and you'll learn that most executives admit to finding it increasingly difficult to build and maintain trust with their customers. So, yes, trust is now a big-time concern for all businesses. You only need to look at the growing number of consumers that are hyper-sensitive to 'data dishonesty', who are walking away from firms they think will abuse their trust.

The search for trust

Consumers are looking for organizations that can reassure them of two things: that they will keep their data from the bad guys, and that they won't use it in ways that weren't intended – something that even big names like Twitter, Amazon and Google have fallen foul of.

In Europe, those two principles are already enshrined in General Data Protection Regulation, but creating trust and transparency shouldn't require legislative pressure, because both are good for business.

If you want to see how this is already playing

out, let's go back a few months to when Apple made app-tracking transparency part of its latest system update, immediately breaking Facebook's ad machine since it could no longer sell targeted space based on what people look at on their phones.

Confronted by the prospect of a potential \$10 billion hit to its sales, Facebook responded by taking out full-page ads in the New York Times, Washington Post and Wall Street Journal, accusing Apple of undermining the 10 million businesses that advertised on its platform.

They may not have liked what happened, but with 85% of users around the world and 96% in the US clicking on 'ask app not to track' when prompted, it's easy to see which way the wind's blowing. Did it cost Apple money? Sure. But if this is a statement of intent to build the Apple brand around privacy long-term – and it seems like it is – then it's going to pull others into the sunlight.

Trying to bury 'awkward truths' in the small print because you know consumers are never going to look there isn't being smart. You're breaking their trust and that's going to put you on the wrong side



“

Creating trust and transparency shouldn't require legislative pressure, because both are good for business.

of history. If that's a place you don't want to be, you are going to have to do some things differently.

First off, if you're still making a product or service, then looking to create a need for it among consumers... stop, because we're no longer in the Mad Men advertising world of the 1960s. Reverse the polarity. Move to where the consumers are and create the product they need. According to research by leading CX platform, Emplifi, 60% of consumers would pay more to get a good customer experience.

An obvious example of this is Starbucks. They satisfied a need by creating a place people enjoyed going socially, and where they could spend \$5+ on a nicely-profitable cup of Pumpkin Spice Frappuccino if they wanted to.

Take it steady

Don't look to move your customer relationship forward too fast, because that's not the way to build trust. If you pretend it's love at first sight and start talking about marriage on a first date, you won't see customers for dust. Instead, start by learning what you both have in common. That's the first rung on the trust ladder. Then slowly get to know each other more. Show that you care, make them feel special, and then go from there.

This might not sit well with your commercial instincts, which tell you to upsell and cross-sell to make more money and get a bigger share of the market. But patience is key. You need to be thinking about customer lifetime value, not instant gratification.

And the only way to build customer loyalty is to get people to trust you long-term. So, if I give you my data and you continually provide me with exactly the product or information I need, when I want it, I'll come to trust you implicitly.

But if, as my bank did, you convince me to switch on my phone's location services on the pretext you're improving my security, but then use that information to push location-based ads for partner products and services without my authority, then we've got a problem. That's not a caring relationship, it's a trust-abusing one.

Who are you?

To build trust, you need to know what your customers want in the first place. And here's where firms using behavioral analytics are at a huge advantage because of the way they can micro-segment their market. Amazon's now using predictive analytics to such an extent

“

Patience is key. You need to be thinking about customer lifetime value, not instant gratification.

that it's shipping your products before you have even ordered them! If you're still relying on demographics, you're not using a precision instrument but a blunt tool.

A couple of years ago a meme was doing the rounds about two men, both born in the same year, wealthy, self-employed, who spent a lot of time in London and liked international travel, dogs, sports cars, fine wines and were also parents and had remarried. You would think that's a comprehensive profile that should get your marketing off to a good start, wouldn't you? But are Prince Charles, heir to the British throne, and the self-proclaimed Prince of Darkness himself, Ozzy Osbourne, lead singer with rock band Black Sabbath, really in the same customer category?

If you want to build trust, here's how: get to know people. Put their needs before yours and don't treat their data as your own. Instead, use it to their benefit and you will be building the long-term loyalty that adds to your bottom line. It's not rocket science, just good business.

For references, please go to cxomag.com/article/trust-or-bust-why-transparency-matters/



With a career spanning 20-years focused on digital experience, design, and innovation **Lisa Woodley** has built and led successful multi-disciplinary teams that deliver innovative experiences rooted in user need, business value, and design ethics. In

her current role as a General Manager for Nexient, an NTT DATA company, Lisa brings the human perspective to technology and innovation to deliver solutions that elevate brands and drive business value. In addition to her role at Nexient, Lisa is Adjunct Faculty at Rutgers University where she teaches User Experience Design in their Master of Business and Science program.

Opinion

Opinion pieces from NTT DATA's
subject matter experts.

In Data We Trust: But Do We?

By Theresa Kushner
Data and Analytics Practice Lead,
NTT DATA Services



Obtaining data can open up a whole wealth of business opportunities, as long as the data is valid and trustworthy. However, having incorrect, outdated or inaccurately sampled data can be damaging and costly. In such turbulent times, how can we secure data integrity for the best outcomes for businesses?

In the last few months, we have seen data used, misused and abused to report on the Covid pandemic. The only consistent opinion of the data that has been shared with the general public is that we're not sure what to believe. Is the virus really that rampant? Do masks really make a difference? How many deaths were caused specifically by the virus?

Data has attempted to answer all those questions, but the answers are still not trusted. So, what difference does it make whether we trust data or not? Why is it important and how do we ensure that the data we use to run our businesses falls into that trusted category?

In Stephen Covey's book, *The Speed of Trust*, he makes the point that 'trust impacts us 24/7, 365 days a year. It changes the quality of every present moment,' he says, 'and alters the trajectory

and outcome of every future moment of our lives.' But, Covey argues, the real reason that we need trust in business is because it contributes significantly to the speed at which we respond to our customers, our employees, and our boards. 'When trust goes down, speed also goes down and costs go up,' he writes.

How lacking trust in data will impact your business

Here are two examples of how lack of trust in data affects the speed of your business.

1. The Revenue Conundrum:

Your business manager has just handed you sales figures for the past quarter. You look at the bottom line and it doesn't seem right. Last month, the revenue figures were off by \$500K. So, immediately you eye this month's figures with skepticism. You don't

believe – or trust – the data. Without hesitation you deploy additional resources from your team to "look into those figures." A few days later the team has pulled together a new report that you think looks closer to what you think it should be. But your team is now days late on another project and the decision you would have made to help generate more revenue has yet to be put into action. And, finally, you have expended resources to do work that had already been done.

2. **The AI Algorithm:** You just finished reviewing the latest results of the Data Scientists' team and the direction that was recommended is exciting. However, when the team explained what they had to go through to get the right data set, you wondered how the team has analyzed the last 5 years of resumes and hiring data from HR to recommend a model for hiring a more diverse employee population. When the project was tested, however, the model recommended hiring individuals that fit the same 'thirty-something, white male,

“

Our study found that 15% of companies don't understand what data they have. The promise of privacy is a good way to evaluate intent. Is the data you are using from reliable sources?

Ivy-League school profile'. The data that the team used was accurate and plentiful but biased toward continuing the same hiring practices.

Ensuring data integrity

Data integrity in today's world is so important because AI algorithms learn from the datasets they initially train on. That learning becomes the basis for additional learning over time. If the initial dataset is not representative of the problem at hand, then the AI algorithm will produce spurious and ineffective information. In fact, this AI example comes from a high-tech company in Silicon Valley who spent four years and millions of dollars on a hiring model that they scrapped as a result of using the wrong data. These are not isolated examples; these scenarios happen in businesses across the world – daily. A recent NTT DATA study found that, while 78% of companies in North America understand the value of their data, only 43% of those surveyed agreed that data plays a pivotal role in the decision-making processes in the company. And both data leaders

and laggards from the study conveyed that “senior leaders not seeing the value of using data” remains a challenge when attempting to derive meaningful value from their data. So, how do you put trust back into your data? How do you get senior leaders to see the value in data and trust it? Using Covey's approach and examples in conjunction with insight from our study, we can look at our data in four ways that help create credibility. What are your answers to these questions?

- 1. Integrity:** Does your data have integrity? Does it truly reflect what we know is reality? Is it current, complete, consistent and accurate to the best of our knowledge? How do we know the data is high quality? What good decisions have we made with the data presented to us? About a third (34.2%) of organizations identify improving data quality as the biggest challenge in managing their data.
- 2. Intent:** What is the Intent of the data? Is the data collected and used in a way consistent with the intention of its use? Unfortunately, our study found

that about a sixth (15%) of companies don't understand what data they have. The promise of privacy is a good way to evaluate intent. Is the data you are using from reliable sources? Do you have the owner's permission to use it? Are you using data collected for sales activities that are now being used for HR activities or vice versa? Does the data fit the intent?

- 3. Capability:** Do you have capable data people? Do you have people who understand the meaning of the data that you use and depend on? Do they understand its lineage, its flow through the organizational applications and its maintenance? Can these people establish and/or restore trust with the users of the information the data provides? About a fifth or 21% of our study respondents don't have the necessary skills and talent to analyze the data.
- 4. Results:** When you use data, do you get the results you want? Does the data deliver quality information consistently? Can you quickly assimilate the information derived from the data and apply it

“

The real reason that we need trust in business is because it contributes significantly to the speed at which we respond to our customers, our employees, and our boards.

to the business decision you need to make? Data gives you information that can be applied to the business. Are you getting value from your information? That's why this step – results – is so important. Our study revealed that only 10% of the organizations use data very effectively for transformational processes, and 17% of respondents say they're not using data effectively at all.

How to establish trust in your data

If you lacked answers or answered negatively to any of the questions above or were hesitant with your answers, you might have an issue of trust in your data. That lack of trust will slow you down and create additional expenses in your organization. Here are some simple actions to take toward establishing trust in your data.

- 1. Assign a data owner.** This owner should be given responsibility for the data, but also the power to act on its behalf. Although you can hire this individual from outside your company, it's often best to

select someone internally who has the trust of your employees and leaders. Trusting the data owner is a first major step to securing trust in the data. And don't make the mistake of thinking that an executive is necessary for this task. We've seen many governance programs led by individuals pulled from throughout the organization. It all depends on the culture of your company. Who do people trust the most? A little over one-third or 37% of our survey respondents say that they have appointed owners for all their data sets.

- 2. Identify a key project.** Identify a key project that links to or contributes to the overall goals of the company. For example, if your goal is to generate 10X the revenue from last year, then use the data to identify what products and channels you will need to expand to reach the goal. Use the data also to tell you where your weaknesses are in the supply chain, the go-to-market and financial operations. Make sure that you always start with the data associated with the process or task. Give it a spotlight so

that, when you reach your goal, data can be a key contributor.

- 3. Develop systems, processes and people.** Only 31% of respondents from our survey say that data is shared seamlessly across the enterprise. This is a big step. You may have systems, processes and people already, but are they tuned to the requirements that you have for a data-driven environment? Do you have applications whose data does not link to or talk to other applications? Do you have processes that are broken or incomplete? Do you have people who understand the data from their area of responsibility, but haven't a clue as to how their data affects the entire organizational process? Trust in data begins with identifying what is leading to the lack of trust, putting a plan in place to correct any issues, and then using data to make business decisions, accelerate growth, save costs and drive employee and customer satisfaction.

Information and Cybersecurity in the UK: The State of Play for Corporates

Ken Jones, Security Consulting, Regulatory Director, NTT DATA and Warren O'Driscoll, Head of Security Practice, Senior Director, NTT DATA UK



The different needs of cybersecurity continue to evolve, in the same way that businesses must adapt and respond to these cybersecurity risks and challenges. Partnerships are just one of the many ways in which businesses can protect themselves and move with the times.

Information and cyber security is one of the hot topics of the last five years, as digital enablement becomes the default and its potential to impact global and UK business continues to grow on an almost logarithmic scale.

The UK government's National Risk Register published last year found that 46% of businesses had reported a cyber security breach or attack over the course of 2020, in addition to 26% of charities. The scope of threat facing corporations in the UK has evolved and grown in recent years; the way companies must adapt to meet this risk needs to change as well. In reacting to these risks we are also seeing revolutionary changes in security and data regulations both at a global scale and within the UK. The Taskforce on Innovation, Growth and Regulatory Reform

recent report indicates a move away from code-based regulation and more towards a common-law approach. This is likely to result in more weight being given to the supervisory judgements of regulators, which could mean more focus on outcome rather than just the process. For UK corporations, this shift in regulatory approach must be considered in context of the regulatory penalties, brand impact and the threats posed to business, shareholders and the client.

With the increase in the cyber security landscape, blurred corporate and cloud data boundaries, and ever increasing threat levels, the UK's position as a tech and services leader makes it a more attractive target for malicious actors than most.

Due to limited effective

understanding and articulation of risk appetite, or the threat impacts to the asset base, at both the executive and board levels, far too many organizations make the mistake of addressing security risks as just an IT function or create security policy in isolation. This often results in complaints that security is too costly or not in tune with the corporate need. While security frameworks and standards offer businesses effective guides to good practice, only effective clarity of the corporate risk appetite, and its relation to its assets and their threat impacts, can effectively dictate and align the control objectives and responses for the individual business.

As per the guidance offered to businesses by a number of the UK Regulators, we need to be challenging boards and executives to firstly have a clear understanding of their business's assets (i.e. people, products, processes, property, data and technology) and where they stand in terms of the corporate risk appetite for impact, from aspects such as threats,

“

A move away from code-based regulation and more towards a common-law approach is likely to result in more weight being given to the supervisory judgements of regulators, which could mean more focus on outcome rather than just the process.

regulations, contractual and certification drivers.

What is the risk?

For around the last ten years The World Economic Forum's Global Risks Report has highlighted the failure of cyber and data security as one of the principal global risks, along with issues facing technological governance and a globally accepted system of regulation regarding critical digital networks and technology. Of global risks surveyed in the 2021 report, only threats relating to public health and climate change were seen to be more of a clear and present danger than cyber security failure.

The cyber threat can take many forms for businesses. The emergence of ransomware-as-a-service allows hackers to essentially auction their skills to the highest bidder, opening the door for those who may wish to carry out attacks but previously did not have the technical skills or capabilities. Phishing attacks have also continued to be a common threat, and the pandemic has seen renewed

acceleration in their frequency. Those carrying out these attacks have sought to play on anxieties and uncertainties generated by the pandemic, attempting to instigate an emotional response that leads to a link being clicked and a breach occurring. And the abundance of digital change without basic security by design or default only makes the lives of threat actors easier.

The corporate supply chain also represents a significant security threat vector. The nature and integration of the supply chains makes it an attractive target for threat actors, as businesses frequently lose sight of the security involved in the process. Research this year found that only 1 in 20 UK organizations take active steps to address the vulnerabilities in their wider supply chain; this is seen as such a concern for UK companies that the government has called for industry input on this topic and will report on its findings later this year.

While these threats are commonplace for mature businesses, there are often still

many gaps between awareness and effective action. Corporations may well inform shareholders about their knowledge of these threats and the principal corporate risks that support them, yet in our experience the evidence of tangible and effective corporate security culture that support the response to these risks is limited and in many cases is little more than a tick box or paper activity. This can lead to risk management or security being seen as a problem when it goes wrong. A greater amount of foresight and appreciation of the risks is needed by executives and boards, not only to protect shareholders, but also the security of customers, staff and the ecosystem as a whole.

How do businesses deal with this risk?

Competitive drivers and business models means every organization has a different risk appetite. Different industries face different regulatory positions, certification and contractual requirements all of which translate into varying levels of organizational pressure.

“

A greater amount of foresight and appreciation of the risks is needed by executives and boards, not only to protect shareholders, but also the security of customers, staff and the ecosystem as a whole.

This variety in risk appetites, methods and operational models needs to be taken into consideration when addressing security risk for individual organizations. There is no one-size-fits-all solution that can be applied to every industry, as each sector will have a different operating model, levels of security maturity, capability, capability and path experience.

For example, the heavily regulated financial services industry will have a very different maturity to construction, where security maturity is not a core competence. Even within these sectors, each business will face a different level of operational and security risk, based on assets and threats, and therefore require an appropriately individualized approach towards risk management.

To address this disparity, the UK's NCSC's National Cyber

Security Strategy has highlighted the importance of partnerships in helping individual organizations navigate a strategy which is right for their specific circumstances.

By engaging in partnerships with core competence and path experience, partners such as NTT DATA can coach, challenge, mentor and advise across all levels of corporate accountability to ensure the unique challenges facing an organization are taken into account, so businesses will be ultimately better placed to navigate the ever-shifting landscape of Information and cyber security.

5 Minutes On...

Cybersecurity and Bridges of Trust

By Martin Stremper
COO, NTT DATA Business
Solutions Brazil



Martin gives CXO 5 minutes on the current cybersecurity landscape, how businesses can minimize the threats associated with new technology and cloud-based services, and why trust between customers and service providers is so important.

Scan the QR code with your smartphone camera



Zero Trust – It Begins With Identity Management

By Christian Koch
Vice President Cybersecurity and Lead for IoT/OT
NTT DATA DACH



Zero trust is a necessary evolution for businesses to be cyber secure in our digital modern landscape. To eliminate cyber risk and threats, businesses can implement a zero trust approach to protect data and systems every step of the way.

The issue of zero trust often appears after the introduction of various cloud applications. In some cases, we also have customers where the CIO or CISO gets questions from the board about cybersecurity, data protection and the risks for the company. They are then asked specifically about their own IT strategy for zero trust.

Whenever data migrates to the cloud – whether Microsoft, AWS or Google – and cybersecurity awareness increases as a result of incidents in the press, at partner companies or even in your own company, the question arises of how to ensure secure access for a distributed environment. Then it

says: we want maximum security, ideally a zero trust architecture. That means that everyone who wants to access data, applications and systems in the cloud and the corporate network is treated in such a way as if they were an untrustworthy outsider.

From now on there is no longer a leap of faith for employees. What does that mean in practice?

Better security, faster

The good news for you is, in the first step, zero trust does not require you to completely rebuild the entire network and cloud infrastructure, nor to carry out micro-segmentation down to the last small segment. Likewise, new

hardware for the entire network does not have to be purchased immediately. And no, there is no need for an assessment of the entire infrastructure in all parts of the company either – unless you want to introduce zero trust according to textbooks, which means that nothing happens for at least a year. By “nothing” I mean: this year your data will not be a millimeter more secure. That’s why we at NTT DATA are tackling the issue pragmatically so that our customers can quickly benefit from more security.

With Zero Trust you can start immediately

So that we don’t misunderstand each other, of course, before every zero trust project, we take stock. Which technologies are in use? Which cloud-based applications? What is the status of authentication? However, instead of examining all aspects of Zero Trust – identities, end devices, applications, network,

“

With a solution-oriented approach, you have more data security with every measure.

infrastructure and data – we build on the basis of Zero Trust, namely the existing identity management with rights, roles, organizational units and suitable strong authentication processes for the users. This forms the basis for Zero Trust.

The second step is then to identify applications and systems that can be easily optimized in the direction of Zero Trust. These mostly include cloud applications, where the microservices can be segmented with relatively simple means, connected to the identity management via a ‘conditional access engine’ and the data can be secured within the application. With this solution-oriented approach, you have a bit more data security with every measure. In good business terms, with our customers, we are getting more and more Zero Trust, quick win for quick win.

As I said, the first thing we do is focus on our customer’s existing identity management.

Experience shows that people often think in black and white, i.e. either no access at all or full data access. This rarely helps data security and data protection. Here it is important to raise barriers according to defined roles and access authorizations and requirements and thus to implement secure, always traceable ‘limited access’.

Securing all data access

To anyone who is now wondering whether it might not be better to convert the entire infrastructure to Zero Trust right away, I would like to answer the following:

If employees access the company’s cloud services from home, then they don’t have any infrastructure operated by you in between. A highly secure company IT structure does not protect the data from access from mobile devices – whether it is on the desk at home, in the ICE on-board restaurant or in the lecture room of a hotel.

A Zero Trust network concept is certainly important and should not be neglected, but it is not the first priority for the project start. Usually there are also dependencies on the hardware or software used and it has turned out to be easier to focus on these topics based on Zero Trust concepts when replacing hardware or software after maintenance has expired. That’s why I advise you: start Zero Trust with identity management and applications where the implementation does not require a complete redesign. For an initial, professional overview, we recommend our Strategic Guide to Zero Trust.

NTT DATA's Zero Trust Journey 1: Blazing the Trail

By Sushila Nair
Vice President, Security Services, NTT DATA Services



There are misconceptions around Zero Trust, as businesses may be fearful of a perceived need to completely rebuild their security architecture, but all it takes is a step-by-step approach. What is the journey to making the security of your business airtight?

It's been said repeatedly: Zero Trust is a journey. The core concepts of the Zero Trust strategy have circulated in the cybersecurity field for decades. Still, until the National Institute of Standards and Technology (NIST) released SP 800-207, there hadn't been an architecture around which to build. It was Forrester analyst John Kindervag who initially coined the term years ago and in the words of another Forrester analyst: Zero Trust is not one product or platform; it's a security framework built around the concept of 'never trust, always verify' and 'assuming breach.' Attempting to buy Zero Trust as a product sets organizations up for failure.

Zero Trust isn't a technology or even a fully codified framework: Zero Trust is a mindset, an approach, a way of viewing

cybersecurity. But as the world has changed in the last few years, it's a view that's taken on greater and greater importance – and global enterprises like NTT DATA recognize that.

"The legacy idea of workers and workloads somehow being more secure just because they are sitting in some brick-and-mortar location was flawed, to begin with," says Steve Williams, Enterprise CISO (Chief Information Security Officer) for NTT DATA Services. "But that model has been thoroughly destroyed by today's business reality, which requires workers to be productive from anywhere, at any time, on any device." He adds, "To either gain or maintain a seat at the proverbial table, CISOs must look to Zero Trust as the means to not only secure their business but also continue

earning the trust of their clients/customers."

With any major undertaking such as this, you need a shared vision and leadership buy-in across all regions and business units. For a large global enterprise like NTT DATA, that means synchronizing multiple CISOs and many regulatory and compliance regimes.

Here is the story of how NTT DATA began our migration from traditional, perimeter-based security to a Zero Trust architecture.

The start of NTT DATA's Zero Trust journey

NTT DATA started its journey nearly two years before the pandemic. "In 2018, it was rarified air to find vendors who were committed to building products that could be fully leveraged in a Zero Trust ecosystem," says Williams. "Even today, Zero Trust remains more of a marketing term than an actual product or practice for many security companies. Fortunately, we've been able to find partners and solutions that have worked well for us and – most important

“

Zero Trust is a mindset, an approach, a way of viewing cybersecurity. It's a view that's taken on greater and greater importance.

– were willing to collaborate in the continuing journey towards Zero Trust.”

“NTT DATA is growing continually, and a significant part of that growth comes through mergers and acquisitions,” says Hiroshi Honjo, Head of Cyber Security and Governance at NTT DATA's Technology and Innovation General Headquarters in Tokyo. “We had a very frank discussion with the board early on, and our position was that the only way we can consistently grow globally and stay secure is through a Zero Trust architecture.”

Any organization's security is only as strong as its weakest links. For an organization like NTT DATA, spanning the globe with so much growth driven by M&A, there are plenty of links to examine. We recognized that we needed a common approach, framework and toolset to secure ourselves globally. We standardized on the NIST CSF and used a Zero Trust framework, paying particular attention to SP 800-207.

“There was some debate, of course,” says Honjo-san.

“Changing from a traditional security architecture to Zero Trust requires significant investment, and the board wanted to see the justification for those costs. But the board ultimately recognized that NTT DATA needs to have security at the highest level globally while still having flexibility – and those were the factors that eventually swayed the board: Zero Trust allowed us to keep the utmost security while having the flexibility to react.”

Understanding the user experience

Zero Trust needs a fundamental shift in how work is performed and how workflows are handled, so we felt it was imperative to chart our journey with the User Experience (UX) at the core. Security of any kind is most successful when it integrates with how users want to perform their duties, rather than forcing them to do something different or new. When security forces users to adopt more difficult or more time-consuming workflows, problems inevitably arise.

“Given the choice between convenience or security, people

will choose convenience 99 times out of 100,” says Williams. “That's not because people are lazy or evil. Rather, people are predisposed towards what psychologists call an optimism bias – the belief that you are less likely to experience some negative impact or event. We all think ‘that won't happen to me’ when we're watching news stories about major breaches.”

We had to design our Zero Trust architecture so that the most secure way to do things was also the most convenient. There's often a disconnect between what technologists envision people doing and what people end up doing.

A classic metaphor for this behavior can be seen every day on campuses worldwide. Brilliant architects designed concrete walkways between buildings that they believed to be the best or desirable paths, yet simply looking at the dirt trails worn through the quads shows how people naturally want to move. These are often referred to as desire paths.

Williams sees this as a challenge rather than an

“

We all think ‘that won’t happen to me’ when we’re watching news stories about major breaches.

obstacle. “The successful CISO will embrace this disconnect and challenge themselves to use this pandemic-induced opportunity for a hybrid work environment to provide security around those natural paths wherever possible.”

A culture of continual improvement

Markus Künzler, EMEA CISO at NTT DATA EMEA Ltd, says that NTT DATA’s global security leaders have not only embraced this challenge but pushed each other to find new ways to meet it. “There has always been a spirit of cooperation globally when it comes to security, but I would say that it’s gone a step further now,” says Künzler. “Now it’s almost a friendly competition among us, all of us trying to find innovative ideas and new techniques and new ways to meet the challenges we’re facing. There’s a real spirit

of the global community when it comes to NTT DATA’s Zero Trust program.”

“Our clients trust NTT DATA to be the trusted global innovator,” says Honjo-san. “And security has to be central to that. So as global CISOs, we have to communicate regularly, talk with each other about the challenges we’re facing, the risks we’re trying to mitigate, and the solutions that have worked for us. NTT DATA has incredible people and cutting-edge technologies at our disposal; it’s our job to ensure that we help build and maintain a culture that allows everything to flourish.”

NTT DATA’s Zero Trust Journey 2: Architecture (and What We’ve Learned)

By Sushila Nair
Vice President, Security Services, NTT DATA Services

The zero trust journey is all about taking measures to assure your business security at every level. While it sounds complex, it is more simple than it seems, and is worth every effort to ensure that access to data is only granted to those who have sufficiently proved their identity at every stage.

Once we’d evaluated our own needs and strategy, and we’d gone through the arduous task of finding vendors who could meet those needs, our Zero Trust path got much smoother. Our journey started with the ‘new perimeter’: identity. We set out to ensure that the right users always have access to systems they need when they need it – while keeping everyone else out.

Identity management

We started our Zero Trust journey with identity. We implemented robust Identity and Access Management (IAM), including identity management workflows, role mining/defining, single sign-on (SSO), and multi-factor authentication (MFA). We then leveraged identity data about systems and users from a diverse range of sources within our ecosystem.

The data integrates with

various endpoints to ensure only the right people gain access. The move is to use a risk-based approach to granting access. If an account has been compromised – or if a user is connecting from a non-corporate device – then the decision around access (and the level of assurance needed to grant access) should reflect the confidence we have that this is a trusted user, and that the level of assurance increases as the perceived risk increases. This kind of architecture requires a well-integrated structure that enables sharing of information and orchestration of response.

The strategy is to use conditional access and private access agents for users and endpoints. This creates an encrypted, end-to-end connection, mimicking a VPN-like ‘bubble’ around our various digital properties and internal systems.

We extended internal servers

and applications to our users via SASE (Secure Access Service Edge) Private Access, setting up our access restrictions such that only authorized endpoints could access systems and data. We use SASE tunnel ranges as well as security technology to ensure our endpoints are not only authorized NTT DATA devices, but they’re protected end-to-end by our SASE solution.

We did not, and still do not, provide our users with privileged access. We have adopted a catalog approach to installing applications, and our service desk uses a PAM (Privileged Access Management) solution to enable JIT (Just in Time) privilege access.

Endpoints and network security

Our endpoints have their own identity and are managed, secured, and monitored via endpoint management solutions, OS (Operating System) and third-party application patch management, the SASE, as well as endpoint detection and response solutions.

Zero Trust isn’t simply about identity and access management from the perimeter: network security is still critical for providing defense in depth. To that end, we installed next-

“

The decision around access should reflect the confidence we have that this is a trusted user, and that the level of assurance increases as the perceived risk increases.

generation firewalls (NGFWs) to take advantage of device filtering, deep packet inspection, and other capabilities. And underpinning everything, of course, we continue to check our entire ecosystem. We make use of extensive vulnerability scanning to ensure all OS and application patches are installed and effective. Finally, all our security systems feed our SIEM (Security Information and Event Management) / UEBA solution to ensure real-time entity behavior analytics, anomalous activity identification, and automated workflows and case management to reduce time to respond.

What we've learned

As with any expedition of this scale, we've taken many lessons from our Zero Trust journey, many of which apply to any organization looking to follow our path.

There are some truly non-negotiable things with any Zero Trust program:

1. Executive sponsorship and buy-in: To weather the inevitable

pushback that will come from across the business units when moving to Zero Trust, the executive team must be aligned from the start. You can't start any journey unless you know where you're headed, and making sure your executive team agrees on that destination is critical.

2. Hygienic Identity: To ensure you can accurately assess and assign each transaction, you need to have a known and trusted source of record.

3. Well-integrated technologies: Zero Trust needs a deep tech stack of security and business solutions working together with one another to send and receive the necessary security signals across various control points.

4. Clear communication with users: No matter how well-designed your Zero Trust roadmap is, your users will experience some changes. You need to ensure your people feel included and educated along the way and understand the reasons they are being asked to change behaviors. It's not enough to simply tell them the 'what,' you

need to give them a meaningful 'why' as well.

5. An abstraction layer: You do not want to be forced into a single (and therefore limited) tech stack, so you need the ability to add/remove/augment vendors as your security and business needs evolve.

In our experience, in practical application, missing any one of these things will lead to failure — or at least a compromised architecture. Beyond these critical factors, there are several "wish list" items that will make the journey much more comfortable and increase your chances of success:

- **Behavioral analytics:** This will provide a more dynamic data set to support the decision-making process as you evaluate and evolve your program.
- **DevOps/DevSecOps:** Having a team dedicated to integration and user experience bug fixes that absolutely will occur during the process will lighten the load for everyone.
- **Self-service capabilities:** Some form of self-service

“

You need to ensure your people feel included and educated along the way and understand the reasons they are being asked to change behaviors. It's not enough to simply tell them the 'what,' you need to give them a meaningful 'why' as well.

dashboard to see what's going on with your user experience and understand what blockers/limitations you are hitting is a major boon. This will help keep your help desk and service teams from being overwhelmed with support calls.

“Designing security based on the risk of an individual transaction, rather than on a giant and often incomplete context, just makes sense,” says Steve Williams, Enterprise CISO (Chief Information Security Officer) for NTT DATA Services. “Unfortunately, it has largely remained an intellectual exercise. Vendors are more than happy to throw 'Zero Trust' around as marketing jargon, but most solutions have effectively no real capabilities or ability to help you develop a true ZTA (Zero Trust Architecture).”

It's up to the security leaders of each organization to set up their own Zero Trust goals and needs, and to work with a provider that has experience in designing Zero Trust programs. Be honest and fearless in evaluating your

own capabilities and those of prospective (and current) vendors. It's not an easy journey, but it's a trip well worth the effort. The world isn't slowing down, nor is the evolution of the threats we all face. Zero Trust is not an end state: it's just the next phase in doing everything we can to ensure our clients, our businesses, our users, and our critical data is as safe as it can possibly be.

Make life easy for customers, not for ID fraudsters

Mickey Nachimovskey
Senior Director, Business Development and Partnerships, NTT DATA UK



Strict ID checks become increasingly imperative in our rapidly evolving digital landscape, but sometimes they can be arduous. How can companies protect themselves and their customers from cyber risk while ensuring their processes are convenient, effective and user friendly?

ID fraud is big business. In one recent example, as published in the Manchester Evening News, the police caught someone using 160 fake identities to buy high-end mobile devices online, but only after the scammer had managed to acquire phones worth more than £250,000.

Faced with this sort of crime, the incentive for organizations to impose strict ID checks is obvious. But if companies make ID checks too onerous, they will deter potential customers and lose business, so tightening up the verification process brings its own risks.

Clearly companies must take care to strike the right balance between the likely cost of fraud and the risk of losing customers.

What's also clear is that the balance has shifted, making it the right time for organizations to think again about upgrading their ID verification procedures.

Shifting the balance

Firstly, while fraud is being committed in person in retail stores, the risk of falling victim to fraudsters is growing fast as more interactions take place remotely. Customers were deserting the High Street in favor of online self-service options long before the pandemic, but it's a trend that has accelerated sharply during lockdown. There will always be some customers who want to meet face-to-face in-store, but that's not where the growth is.

Secondly, recent developments

mean that technology is now available to help organizations make effective ID checks relatively painless for their customers. Armed only with a valid photo ID and a mobile phone, it should now be possible to verify someone's identity online in under half a minute.

This is a step change in convenience compared to, say, having to turn up in person at a store or (as required by regulators in some European markets) wait at home for hours for a courier to verify your ID face-to-face when they make a delivery – even if it's just a new SIM card.

Where we are now

Some organizations are ahead of the game, such as challenger banks and fintechs. Some public sector organizations are also on board. For example, UK residents already need a photo ID to sign up for the NHS app that provides proof of vaccination.

However, many other organizations are just waking up to what's now possible. These include traditional banks

“

Details of the procedure can vary to meet the needs of organizations in industries with specific rules on compliance, such as insurance or finance. The entire process is GDPR compliant too.

and telcos, among others. NTT DATA has researched the market and found a best-of-breed solution that can bring these organizations rapidly up to speed. We can also provide all the integration and related project management services to ensure a smooth transition.

The customer experience of ID verification

From the customer point of view, ID verification couldn't be easier. Using any device with a camera (mobile phone, tablet, laptop or kiosk, for example), simply upload a photo of your ID and take a selfie. You may be asked to say a random phrase while you're on camera, but that's it.

All the really smart stuff takes place in the fully automated back end.

1. The system initiates liveness detection to assess whether the images are live and taken in real time, perhaps using the spoken phrase or by looking out for blinking or other movements.
2. It also checks that the ID

document is genuine. UK passports and driving licenses are commonly used, but the system supports thousands of different documents and versions from more than 200 countries globally, so you can also use a residence permit or overseas passport, for instance.

3. The system then uses facial recognition to match the person in the selfie to the photo on the ID.

The whole process takes just a few seconds. The company gets a full report and the agent – human or automated – gets a summary with one of three outcomes: the ID has been authenticated, more information is needed or the application seems fraudulent.

Details of the procedure can vary to meet the needs of organizations in industries with specific rules on compliance, such as insurance or finance. The entire process is GDPR compliant too.

But the real proof of the system's success is that 93% of people agree to go through with the automated process when they're offered the opportunity, rather than opting for a more traditional alternative such

as visiting a store or, worse still, dropping out and not coming back.

Making ID checks work for you

The UK has historically taken a more relaxed approach to ID authentication than some of its European neighbors. This has left some of the country's big-name telcos and banks lagging behind the curve, but that is about to change.

NTT DATA is seeing an upsurge in clients asking for a solution. A combination of our industry knowledge and our proven approach to project management and integration enables us to offer an effective solution that can usually be up and running within three months.

Perhaps the balance of risk for your business means you still want to allow most of your customers free access without ID checks getting in the way? In that case, you can opt to start by applying ID checks only to high-value or especially sensitive transactions. Starting now will set you up to adapt quickly and roll the solution out to smaller transactions when you're ready.

Protecting Customer Accounts and Information in a World of Digital Connectivity

Edmund Tribue
Risk and Compliance Practice Leader,
NTT DATA Services



Strict ID checks become increasingly imperative in our rapidly evolving digital landscape, but sometimes they can be arduous. How can companies protect themselves and their customers from cyber risk while ensuring their processes are convenient, effective and user friendly?

The digital revolution prompted widespread headway for businesses, from automating manual tasks and increasing efficiency to enabling more advanced security and safeguarding data. With all the benefits of technological progression come associated risks. The ability to quickly install new platforms parallels a cybercriminal's ability just as quickly to install harmful malware. The dissemination of accessible consumer data used to inform customer journeys also creates heightened vulnerabilities to mass data breaches and account takeovers.

Data breaches are at an all-time high, and modern platforms and ecosystems are essential to monitor your organization,

identify suspicious activity and rank risk. As a result, CROs and CISOs must focus on solid risk planning and cyber security initiatives to realize the value of cloud computing, remote access, and other digitization efforts while offsetting the associated risks.

What are the key risks right now?

A lot has changed since 2020. Accelerated digitization ignited the corresponding influx of more intelligent, agile, and damaging cybercriminals. Regulations changed seemingly overnight to monitor increasing instances of fraud. One in five consumers experienced online shopping fraud in 2020. Additionally, 72% of online merchants recorded an increase in fraud attempts, a third

of which reportedly lost 5-10% of their revenue to fraudulent activity.

The Office of the Comptroller of the Currency (OCC) and the other Federal Financial Institutions Examination Council (FFIEC) members issued guidance addressing authentication and access to financial institution services and systems. The cybersecurity threat landscape continues to present significant risks to financial institutions, reinforcing the need for financial institutions to effectively authenticate and control access for users and customers to protect information systems, accounts, and data.

In addition to an increase in fraudulent activity, companies are facing another threat: account takeovers. A global survey finds that 71% of cloud users suffered not one but seven account takeovers in the last year alone. Three in every four companies have experienced a malicious account takeover and risk losing revenue, customer loyalty, and a favorable brand reputation. In response,

“

Three in every four companies have experienced a malicious account takeover and risk losing revenue, customer loyalty, and a favorable brand reputation.

organizations are scrambling to identify and intercept fraud and attacks by reviewing outdated systems and processes, upgrading technology, and shifting priorities and budgets.

How can CISOs better protect customer information and accounts?

Basic digital hygiene is an effective way to mitigate attacks and adhere to regulatory requirements. There are eight essential steps every CISO must follow to monitor threats and protect customer information and accounts.

1. Be transparent about how you use customer data

Customer experience drives products, services, and organizational success in today's market, and data transparency is imperative to customers. Organizations that prioritize data privacy earn the trust and loyalty of consumers. In one example of transparent data use, the forward-thinking tech giant Apple held a Data Privacy Day to raise awareness of the importance of protecting data. Apple released the video, "A Day in the Life of Your Data," and showed consumers how they use their

information and how it travels to third-party vendors and websites.

Other companies follow suit and provide consumers with more information about how, why, and where their data is used. Transparency around data use promotes loyalty and gives consumers the insight they need to be active participants in protecting their accounts and information.

2. Review your privacy policy

Global privacy laws legally require privacy policies if you collect or use personal information and consumers expect to see them. Complying with privacy measures enable businesses to follow best practices and maintain compliance across state and international laws. As your business grows and evolves, your privacy policy must undergo consistent review and revision. Schedule a regular, automated period dedicated to updating your organization's privacy policy to enhance compliance.

3. Update software regularly

Outdated applications contain gaps that can be accessed and leveraged by criminal actors. Organizations that delay updating software and fail to replace legacy systems put their assets,

customers, and brand at risk. Naturally, organizations prefer to prioritize updating and upgrading technologies during slow periods, but nefarious characters capitalize on this familiar pattern.

During the Covid-19 pandemic, cybercriminals disproportionately targeted the healthcare and pharmaceutical industries. These organizations were overwhelmed by the influx of activity spurred by the pandemic, and as a result, the organizations that procrastinated on implementing updates suffered higher instances of cybercrime. For example, NTT Ltd researchers identified Drupal, Apache, and Microsoft products as accounting for 72% of vulnerabilities targeted in healthcare.

4. Always encrypt user data

Less than half of businesses encrypt user data. Companies that fail to use encryption are risking their organization and their customer's private information. Most payment providers require retailers to encrypt card details by default during the transaction process, but some businesses fail to prioritize encryption without this requirement. The payment process is streamlined to enhance the customer experience, but companies must match ease-of-

“

Organizations must eliminate ‘swivel-chair’ interfaces that require manual data entry and instead adopt modern platforms and intelligent automation.

use with the latest encryption technologies. Encryption ensures personal information is unreadable to hackers in the event of a theft.

5. Modernize platforms and processes

Heavily manual systems and inconsistent processes are putting organizations at risk. Organizations must eliminate ‘swivel-chair’ interfaces that require manual data entry and instead adopt modern platforms and intelligent automation. Operational risk management helps businesses safeguard weak controls, enhance performance, and prevent unintended consequences facilitated by outdated systems. NTT DATA identifies a mature and optimized organization with a score between 5.00 and 5.99 as one that uses:

- Process: Mature and automated workflows
- Metrics: Fully automated reporting
- Tools: Integrated platform with automated correlation.

6. Educate employees on best practices

It’s not enough to upgrade your technology and platforms without

the appropriate measures to train employees to adopt new working methods. Training and new skilling programs educate employees about identifying and avoiding fraudulent activity, from email phishing scams to unreliable network use.

Organizations should continue to educate employees on evolving Covid-19 relevant cyberattacks and consider establishing their internal communication mechanism or clearinghouse for official Covid-19 news to help reduce employees’ exposure to malicious sites and disinformation. Humans are unpredictable, and a cybersecurity education program can better position an organization to protect its data from the inside out.

7. Test for unseen weaknesses

Numerous cyberattacks attempt to take advantage of lapses in security preparedness. With the rise in hostile cyber activity, it’s more important than ever that organizations prioritize the timely application of patches and updates. For example, if your organization frequently uses a flexible meeting or communication enablement

application, always run the latest versions, and monitor for updates. Beyond that, organizations should prioritize good backups and emphasize end-point control, including appropriate antivirus software. Cybersecurity experts or ethical hackers can audit your website and applications to identify unseen vulnerabilities and tell you areas that need updating.

8. Create a disaster recovery plan

Despite all your best efforts, CISOs and organizations must prepare for the worst-case scenario. You must develop a Disaster Recovery Plan and employ remediation to bounce back quickly from an unforeseen data breach or account takeover.

Naturally, you will always want to intercept instances of fraud, but no industry or organization is immune to experiencing a cyberattack. Therefore, creating a strategy and a backup plan will allow you to remain proactive and agile in the face of risk, protecting your business and its customers.

5 Minutes On...

Customer Experience You Can Trust

By Alin Cuciureanu
Product Owner MES, NTT
DATA Romania



Scan the QR code with your smartphone camera



Understanding the customer helps your organization to create meaningful and valuable experiences. This, in turn, helps to generate customer trust and engagement that lasts.

Tech for Good

NTT DATA uses its technology and innovation capabilities to help its communities and clients.



VIDEO

Keeping People Safe During a Pandemic – NTT, Laboratoires Réunis and AWS

When Covid's first wave swept through Europe, the government of Luxembourg, the Luxembourg Institute of Health and Laboratoires Réunis had to act quickly to find a solution. Using multi-cloud expertise, Laboratoires Réunis and NTT worked together to provide systems that could process over 20,000 daily nationwide Covid tests.

Scan the QR code with your smartphone camera



VIDEO

Inspiring and Growing Female Tech Talent – NTT and Michigan Council of Women in Technology Foundation

The collaborative efforts of NTT and non-profit Michigan Council of Women in Technology (MCWT), which aims to nourish women's tech talent, delivered a fabulous online event, replacing MCWT's annual in-person networking conference that was threatened to be canceled due to Covid-19. The result was a hugely innovative platform that increased MCWT's reach globally.

Scan the QR code with your smartphone camera



NTT DATA Consulting Leadership Team

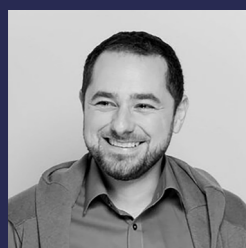
To discuss the CXO Magazine, or NTT DATA's services, please contact one of the leadership team below.



Felice Chierichetti
Head of Consulting,
NTT DATA Italia
felice.chierichetti@nttdata.com



Tim Bardell
Head of Consulting,
NTT DATA UK
tim.bardell@nttdata.com



Stefan Bogdan
Global Head of Consulting,
NTT DATA Romania
stefan.bogdan@nttdata.ro



Sebastian Solbach
Head of Business Consulting
& Solutions, NTT DATA DACH
sebastian.solbach@nttdata.com



Dan Albright
Global Head of Consulting
& Marketing Director, NTT
DATA Services
Dan.Albright@nttdata.com



Stefan Ellerbrake
Executive Vice President
and Head of Global Field
Consulting Services - NTT
DATA Business Solutions
Stefan.Ellerbrake@nttdata.com



The logo features the text "NTT DATA" in a bold, white, sans-serif font. The "T"s are stylized with a gap in the middle. Below it, the tagline "Trusted Global Innovator" is written in a smaller, white, sans-serif font.

NTT DATA

Trusted Global Innovator

© 2022 NTT DATA UK Limited (an NTT DATA company)