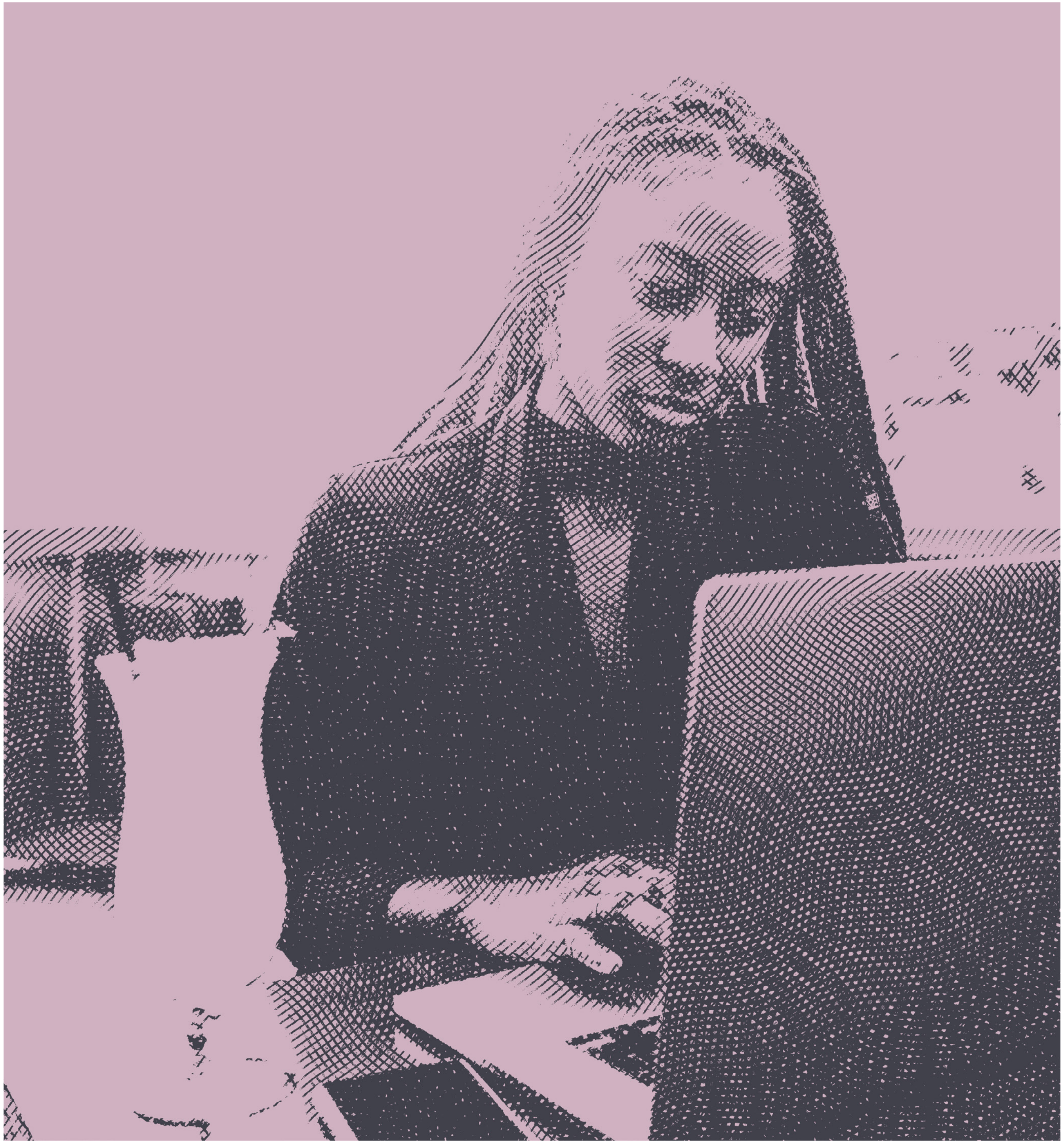
The Okta Digital Trust Index

Exploring the human edge of trust in a fast-changing world



okta

Contents

> “
>
> Trust is a confident relationship with the unknown.
>
> Rachel Botsman, Trust Fellow at
> Oxford University’s Saïd Business School

Introduction

Trust begins with security

The events of 2020 pushed the notion of trust to the forefront of all our lives. Almost overnight, it turned trust in governments and institutions into a consequential matter for most.

It made customer trust in brands acutely important to the bottom line amidst a severe economic recession. And it has forced many organisations to overcome long-standing objections, to trust their employees to work from home (WFH) and to trust digital channels as the only way to serve their customers.

All this comes amidst a backdrop of rising security concerns, triggered by never-seen-before data breach volumes and cyber-threat activity, rigorous regulatory enforcement of data protection legislation, opportunistic social engineering scams, and soaring privacy expectations among consumers.

According to an **INTERPOL assessment**, phishing fraud has risen by 59% in the wake of the pandemic, along with increases in malware, ransomware, malicious domains and fake news, as criminals look to exploit the fear and uncertainty caused by the unstable social and economic situation.

For businesses, security starts with trust. That is, to drive effective security you must first understand as an organisation which employees, partners and customers outside the traditional, office-centric perimeter you can trust to access sensitive data and systems.

However, the reverse is equally true: trust begins with security. In other words, the best way to drive trust among those key stakeholders is to offer effective security tools and policies – especially those focused on seamlessly managing the identities of users.

This is the quickest route to enhancing productivity, and building loyalty and engagement – not just among employees and partners but also customers.

To find out more, Okta commissioned this new survey of more than 13,000 office workers, including over 2,000 in the UK, to help answer the following questions:

How much of our trust is built, maintained and broken in the digital world?

Outside of human connections, how much do we trust when we only engage through our screens?

What external factors are changing our willingness to trust through digital channels?

Are brands, businesses and governments doing enough to build trust?

What follows is the Okta Digital Trust Index: our report exploring the human edge of digital trust in a world increasingly shaped by the effects of the pandemic. We conclude with recommendations for individuals, companies and public organisations on how they can build and deliver real, human trust.

Methodology:

All figures, unless otherwise stated, are from YouGov Plc. Total sample size was 13,163 office workers from the UK, the US, Australia, Germany, France, Italy, Spain, Sweden, the Netherlands and Japan.

This included 2,041 office workers from the UK. Fieldwork was undertaken between 26th November - 10th December 2020. The survey was carried out online.

> “
> Trust arrives on foot,
> but leaves in a Ferrari.
>
> Mark Carney, while Governor of Canada’s central bank (2008-2013)

Section One

What makes consumers trust brands?

In 2020, with the inevitable shift to remote working, office workers also became digital-savvy consumers, spending a lot more time and money online. In the UK alone, consumers **are predicted** to spend over £141 billion on Internet shopping alone this year, up nearly 35% from 2019.

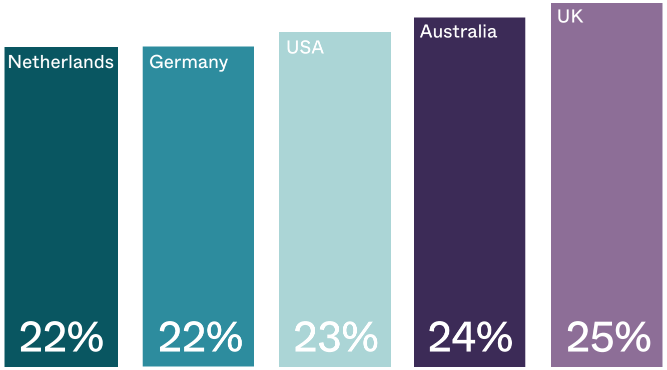
With 2021 being a year of transitioning to more institutionalised online practices, brands are challenged to confidently build new trust and loyalty models with their stakeholders.

Trust is hard won but easily lost today, and although ethical values are increasingly prized by shareholders, investors and boards, we found that when it comes to customers, getting the basics right is more important.

39% of UK and global respondents said service reliability was the criteria most likely to make them trust a digital brand—things like ensuring items arrive on time and in good condition.

Security was also key for them: a quarter (25%) said that having secure log-in options such as multi-factor authentication (MFA) and other measures in place would help to nurture trust in the brand.

This necessity for security was further felt by respondents in Australia (24%), the US (23%), Germany (22%) and the Netherlands (22%).



Percentage of those surveyed who believe having secure log-in options such as multi-factor authentication (MFA) would help nurture brand trust.

Breaches matter

That's not to say that ethics don't matter at all: 8% of UK respondents cited this as the most important factor in driving trust. They also play a big role for consumers in deciding which brands not to do business with – specifically in terms of 'data ethics'.

The top two attributes cited by respondents as making them most likely to distrust a brand were:

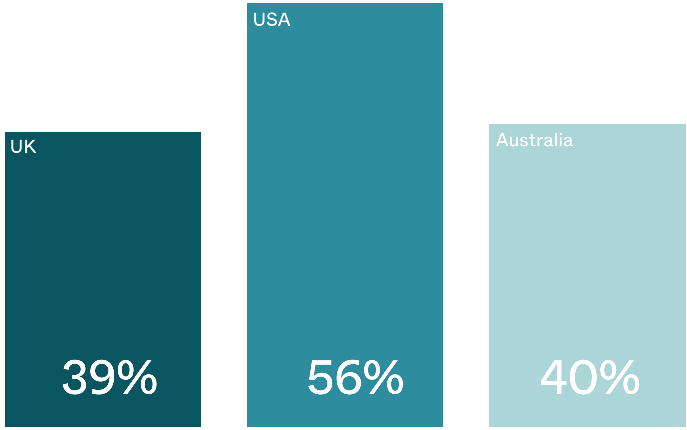
Intentionally misusing or selling personal data	47%
Data breaches	17%

Both are not only a matter of ethics for digital brands but practices that would also draw the ire of GDPR regulators in the UK.

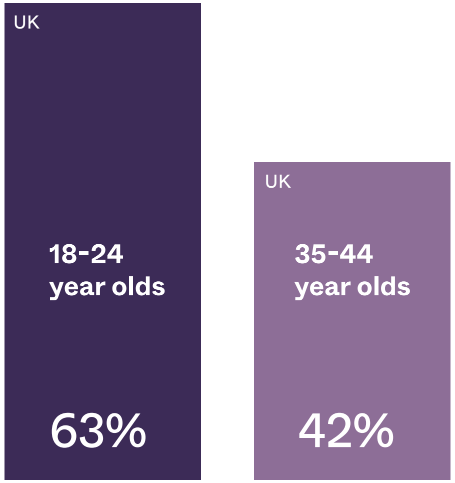
To escape the wrath of customers and a potentially major reputational and financial fall-out, organisations must ensure their data security is fit-for-purpose – starting with best practice identity management.

The intentional misuse or selling of data similarly presented itself as the top attribute for distrusting a brand by all other markets. But while data breaches were the second highest concern for respondents in countries including Australia (16%), the US (15%) and the Netherlands (13%), inconvenience or errors were a more prominent factor in breaking trust for those in France (23%), Spain (21%) and Sweden (16%).

This presents itself as another stark reminder that while data ethics remain of the utmost importance, seamless customer service must not be forgotten.



Percentage of those surveyed who had lost faith in a company due to a data breach or similar.



Percentage of those surveyed who permanently stopped using a firm's services following a breach.

When trust is broken

It's clear that trust is vital for digital brands to succeed in today's highly competitive business landscape.

88% of UK respondents said they would be unlikely to purchase from a company that they didn't trust.

64% admitted that they would have serious reservations about shopping on a website they'd never heard of before.

Once they've gained that trust, brands should be in no doubt that they must work hard to retain it, and that effective cybersecurity is key to them doing so.

Nearly two-fifths (39%) of UK respondents said they'd lost faith in a company due to a data breach or similar. This figure was even higher in the US (56%) and Australia (40%).

Following this event, nearly half (47%) of UK users permanently stopped using the company's services and 36% deleted their account with the company. Even more (52%) changed user settings such as passwords and email addresses, highlighting the importance of secure log-ins to maintaining ongoing trust.

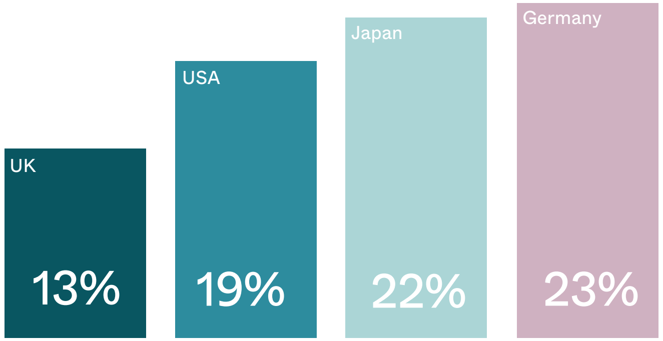
Interestingly, younger UK respondents have a lower tolerance for poor data handling and security from the brands they shop with. Some 63% of 18-24 year-olds said they'd permanently stopped using a firm's services following a breach, versus 42% of 35-44 year-olds.

Given that younger generations will become the growth engine of tomorrow's economy, brands must ensure their business priorities are aligned with these heightened expectations of cybersecurity.

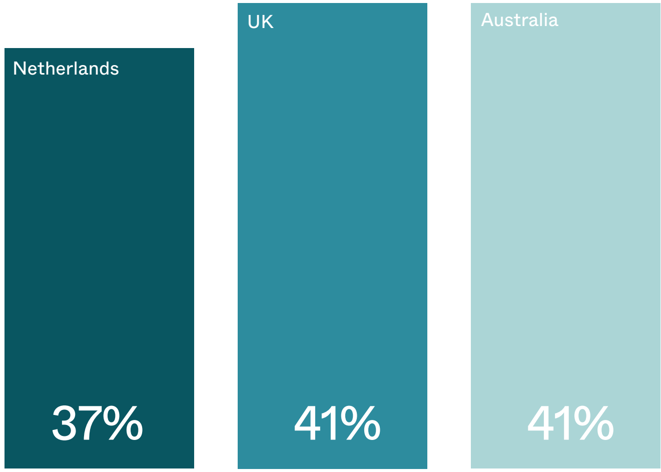
> Younger generations will become the decision makers of the future, so it's important to make preparations and ensure good service and cybersecurity is at the heart of operations to align customer needs with business priorities.
>
> Jesper Frederiksen, VP & GM EMEA, Okta

Much work to do

There's still a great deal of work to do. A significant minority of 13% of UK respondents said they don't trust any digital channels to safely handle their data, similar to those in Germany (23%), Japan (22%) and the US (19%). And it was clear that workplace communications apps (13%) are more trusted than personal ones (4%).



Percentage of those surveyed who don't trust any digital channels to safely handle their data.



Percentage of those surveyed who believe government websites were the most trustworthy.

Most trustworthy of all digital channels in the UK was government websites (41%). This was felt equally by respondents in Australia (41%) and the Netherlands (37%).

This is undoubtedly a positive. Despite initial concerns over handling of citizens' COVID-19 and personal data, there haven't been any major breaches to date, and continued scrutiny appears to be driving improved standards of data security.

> It is so interesting, and encouraging, to see that respondents place government websites as most trustworthy. Research often shows that our trust in the government is declining, but there is a difference between the government (linked to politicians and political parties) and government services (linked to the public sector). This research shows that people trust the institutions of the government, the public sector and government services.
>
> Dr Jessica Barker, Cyber.UK

Section Two

How the pandemic has changed user behaviours

53% Over half of UK respondents said they 'always' or 'often' work from home today, and these same employees will demand more flexibility in WFH policies once the crisis has receded.

Yet whilst isolated at home, many have been exposed to an uptick in cyber-threats aimed at stealing both their corporate log-ins and personal identity data.

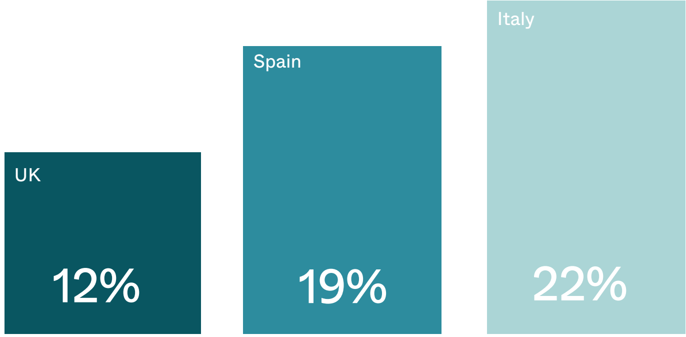
Phishing has become the preferred tactic of many cyber-criminals over 2020. They've had major success using the lure of information on COVID-19 vaccines, or urgent (but fake) updates from trustworthy institutions like the WHO, to trick recipients into clicking through. **Back in April, Google alone said** it was blocking 18 million daily malware and phishing emails related to COVID-19.

As a result, it's perhaps not surprising that 40% of UK respondents said they have become more cautious about providing personal information about themselves online, with just 1% claiming they are now less wary of doing so.

WFH has also made respondents more wary of phishing emails (30%), data breaches (34%) and even AI-generated 'deepfakes' used to spread false information (22%).

26% Respondents feel they're most at risk going forward from identity theft, which is understandable given the increase in phishing attacks many have been subjected to.

Malware (19%) and data breaches (18%) rounded out the top three concerns.



Percentage of those surveyed who believe password theft posed a worry.

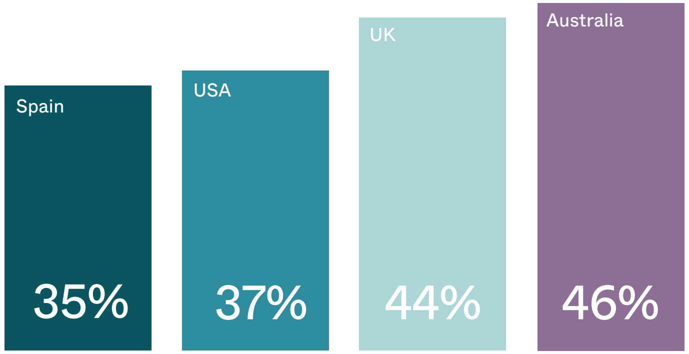
While password theft posed somewhat of a worry for 12% of UK respondents, office workers in Italy (22%) and Spain (19%) felt significantly more at risk from this, demonstrating that the journey to passwordless authentication will only become necessary.

It's worth remembering that an individual may be exposed to cyber-threats not only via attacks targeted at themselves and their devices, but also their flatmates, who may engage in risky behaviour online.

> The threat profile when working from home is heightened for multiple, complementary reasons. People have found themselves sharing devices and home networks as well as physical spaces, increasing risk and compromising written material and confidentiality of audio calls.
>
> Current 'co-workers' can vary from trusted family to barely known flatmates, while the security of having colleagues and an IT helpdesk on hand is removed. To add to this, the behavioural and security mindset that workers previously adopted can be unconsciously compromised when juggling both work and home commitments.
>
> Ben King, CSO EMEA, Okta

Time for transparency

The main reason given by UK respondents for their increased caution online during the pandemic was media coverage about online threats (44%), the same for those in Australia (46%), the US (37%) and Spain (35%).



Percentage of those surveyed who believe media coverage about threats increased their caution online during the pandemic.

While it's great to see journalists playing their part in educating the public, there's a clear opportunity here for digital brands to improve awareness of such issues among customers, thereby building trust. By combining these efforts with tools such as MFA, they can provide greater assurance to nervous consumers – driving revenue and competitive differentiation.

Equally, there's a role for employers here. By enhancing awareness-raising, updating legacy tech that may be vulnerable to online threats, and demonstrating the effectiveness of security measures like endpoint anti-malware, they can give workers confidence that they are as well protected at home as in the office. This benefits not only third-party digital brands indirectly, but also their own organisation: driving up trust in the tools employees use to WFH will ultimately help to enhance productivity.

Section Three

How are organisations responding?

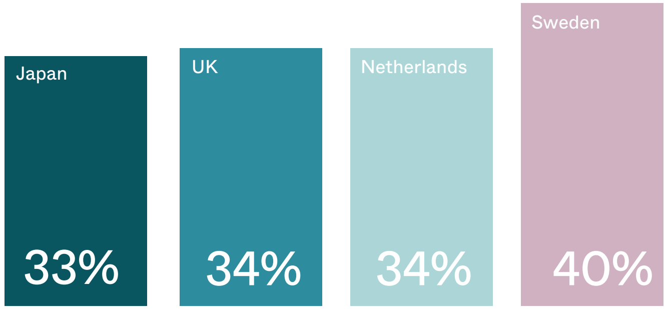
Many employers have indeed taken steps to tackle the growth in cyber-threats facing their home workers. New security applications and technologies like MFA (29%) were the most popular measure, followed by enhanced training for staff (24%). Both are vital in helping to drive the employee trust on which successful businesses are built.

However, more concerning is the fact that 22% of respondents claimed their employer has done nothing so far to combat a pandemic-related surge in online threats. This rose even higher in the real estate (52%), media and marketing (36%) and arts and entertainment (36%) sectors.

> “
>
> For industries that aren’t digitally native, employees often find themselves working from a lower technical baseline, meaning they may not notice or reflect on controls being added to combat online risks. Those that have traditionally faced higher levels of cyber threat, such as banking, technology and retail, would have also likely had a proportionally larger security budget than other industries surveyed.
>
> Across all sectors, CIOs and CSOs have had to divide their time between supporting industry-specific needs and facing security demands, often two very different tasks.
>
> Ben King, CSO EMEA, Okta

What’s more, over a third (34%) of office workers told us they didn’t know one way or the other whether their employer had taken proactive security steps, with a similar sentiment felt by those in Sweden (40%), the Netherlands (34%) and Japan (33%).

This is particularly disappointing as it points to a lack of transparency between business and IT leaders and their employees. You could be running the best cybersecurity systems in the world, but if staff don’t know about it, your business will not be able to foster greater trust with its staff.



Percentage of those surveyed who didn’t know if their employer had taken proactive security steps.

> “
>
> Cyber attackers are always learning new tricks, and workers are aware of this, with many becoming more wary of phishing, data breaches and new risks like deepfake fraud. Businesses must therefore ensure they are staying ahead of the game as much as they can and combat these new threats with new approaches.
>
> Ben King, CSO EMEA, Okta

It’s clear that, if they haven’t already, IT leaders must start rolling out seamless, risk-based identity management solutions to drive trust-based security in 2021 – to enhance staff productivity and minimise cyber risk. Further, they must be more transparent about any new technologies and the security policies they’re designed to support.

Section Four

Conclusions and recommendations

IDC defines trust[1] as the condition that “enables decisions to be made between two or more entities, reflecting the level of confidence between them,” and is an “up-levelling of the security conversation to include attributes such as risk, compliance, privacy, and even business ethics”.

It’s a concept no IT or business leader can ignore today, as digital transformation both expands the cyber-attack surface and simultaneously opens new channels to engage with customers and support employees. When done right, trust will not only mitigate harm, but drive revenue and value for organisations.

In the enterprise it begins with a Zero Trust approach focused around identity, and the ultimate goal of risk-based access policies, continuous and adaptive authentication and frictionless access.

The pandemic has accelerated the need for such approaches so that organisations can trust their remote users are who they say they are, as imposters try in greater numbers to infiltrate corporate networks. It’s also necessary to foster trust among employees so they can work more productively.

But the notions of trust also extend to customer interactions. Today’s digital-first businesses need to constantly nurture that trust as responsible stewards of customer data.

Doing so will drive loyalty and success, even as data and identity thieves stepped-up their own efforts during the pandemic. In this context too, trust begins with security, with identity as its central pillar. That means digital brands providing their customers with the tools they need to authenticate seamlessly and securely.

[1] IDC Perspective, 2020, Future of Trust: Defining Trust, April 2020, #US46185920

Key recommendation summary

Business/IT leaders must be transparent with remote working employees about the cybersecurity measures and policies they're implementing, to foster trust and staff buy-in.

Demonstrate the effectiveness of security measures to remote workers to give them confidence that they are protected as well at home as in the office.

New security tools like MFA and biometrics for passwordless authentication are vital to protecting against consumer identity theft and securing remote access for workers.

Governments and digital services need to continue prioritising cybersecurity and privacy measures to keep citizens' data safe through the pandemic and in the new normal.

More internal training on phishing protection and security best practices are needed to mitigate remote working risks.

Data ethics are important to customers, so businesses must ensure they are adhering to regulatory guidelines, preventing misuse and reducing the risk of breaches.

Keep your security strategy up to date to ensure it takes account of the shifting threat landscape, regulatory risk environment and attitudes to trust.

Ensure your organisation meets the heightened security and privacy expectations of younger consumers, to foster loyalty among an economically important group.

> “
>
> Trust is a human impulse – a precious, beneficial and risky one – and like many of our impulses it can seem hard to comprehend. This fascinating research helps us understand digital trust at a time when the world is rapidly changing and our trust has been shaken, even in something as fundamental as the air we breathe.
>
> These findings show that people don't trust based on words, they trust based on actions. From a cyber security perspective, this reinforces the importance of security as a business enabler, at a time when business continuity and resilience is so important.
>
> The findings also highlight the importance of trust in security culture: the need for organisations to be transparent with employees, customers and the media has never been more evident. Moving forward, leaders cannot ignore trust or they, and their organisations, will be left behind.
>
> Dr Jessica Barker, Cyber.UK

Section Five

Securing the future enterprise with Okta

Identity is the foundation to build trust-based, secure organisations. With the Okta Identity Cloud, business leaders worldwide can confidently create the best digital experiences for their employees and customers.

Secure your employees – wherever they are – with **Okta's workforce identity solutions.** Get the tools to secure and automate cloud journeys, with full support for hybrid environments along the way.

Use Okta's **customer identity solutions** to build secure, seamless customer experiences that your developers and users will love.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organisations to securely connect the right people to the right technologies at the right time.

With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 9,400 organisations, including Engie, JetBlue, Nordstrom, Takeda Pharmaceutical, Teach for America, T-Mobile and Twilio, trust Okta to help protect the identities of their workforces and customers.

okta.com/uk

okta