

STATE OF DIGITAL TRUST

PILLARS OF TRUST

C-LEVEL, DIRECTOR
MANAGER INSIGHTS

DIGITAL TRUST READINESS
SCORE

1245.54°
753234.72°

IDENTITY

AUTOMATION

433.6°
24567.76°

ID 7021.4

THREATS

ZERO TRUST

NOVEMBER 2022

digicert®

GLOBAL STUDY

ENTERPRISES
EMPLOYEES
CUSTOMERS

6578.854°
6765.77°

IoT

XX
SECURITY ALERT



DIGITAL TRUST SURVEY REPORT 2022

We are quickly transitioning from an in-person world to an always-on, digitally connected world. Digital transformation is driving this. So has the pandemic. But how do we establish trust in this new world? How do we:

- Make sure the people (and devices) we're connecting with are legitimate?
- Know that the data we consume is safe?
- Ensure we're not subject to security breaches or denial-of-service attacks?
- Make sure the applications and services we run haven't been compromised?

It isn't easy. This new world has vastly expanded threat surfaces, and the costs of lapses in security have exploded. Especially when you consider that beyond legal, regulatory and remediation costs, the biggest cost may well be a loss of customer loyalty and the company's brand. A Forbes Insights report found that nearly half (46%) of all organizations have experienced reputational and brand damage due to a third-party security breach¹.

This has thrust the issue of digital trust into the foreground. According to Jennifer Glenn, Research Director for IDC, digital trust is the foundation for securing the connected world and necessary for organizations looking to ensure that its customers, employees and partners can be confident that online business processes and interactions are secure.

In essence, digital trust provides the freedom to fully participate in the digital world.

DigiCert, the leading global provider of digital trust, enables individuals and businesses to engage online with the confidence that their footprint in the digital world is secure, has a stake in better understanding how global organizations perceive digital trust and how far along they are in their digital trust efforts.

The DigiCert 2022 State of Digital Trust survey explores where enterprises, employees and consumers around the world have embraced digital trust.

¹The Reputational Impact of IT Risk – Forbes Insights

What is digital trust?

According to Jennifer Glenn, Research Director for IDC, digital trust is the foundation for securing the connected world and necessary for organizations looking to ensure that their customers, employees and partners can be confident that online business processes and interactions are secure.

The foundation of digital trust rests on four key building blocks:

1. Standards that define what the requirements for trust are for a given technology or industry.
2. Compliance and operations that generate or verify digital certificates establishing trust (through identity, integrity and encryption),

with the assurance that these meet the requirements set forth by standards bodies.

3. Trust management that ensures that companies are successfully managing certificate lifecycles and have centralized visibility and control over their use.
4. Connected trust that extends trust throughout more complex supply chains (as occurs with software, devices and content).

Digital trust is derived from these four key building blocks. Companies may rely on third parties for some or all of these activities or manage them internally.

“Digital trust is the foundation for securing the connected world.”

—Jennifer Glenn,
Research Director, IDC



DIGITAL TRUST MATTERS

The need for digital trust has struck a chord with the respondents, as 100% of enterprises say digital trust is important and most (90%) say it is extremely important. So important, in fact, that nearly two-thirds have switched vendors after losing trust in that vendor. And nearly all (99%) enterprises believe it is possible that their customers would switch to a competitor if they lost trust in the enterprise. Nearly half (47%) believe that outcome would be likely.

Enterprise employees are also all-in on digital trust, with 100% saying it is important, and 86% saying digital trust is extremely important. In their roles within the enterprise, 99% would consider switching vendors if they lost trust, with about half (51%) saying switching would be “likely.”

And, finally, two-thirds (68%) of consumers say digital trust is important, with a third (36%) saying it is extremely important. In fact, half (47%) have stopped doing business with a company that lost their trust in the past. Going forward, 84% would consider switching, with 57% saying switching would be likely. Notably, the wealthier consumers are, the more they say digital trust is important (58% of consumers with above-average income say digital trust is important).

Methodology


Dallas-based Eleven Research fielded the 2022 State of Digital Trust survey in September 2022. The survey was administered as a phone and email survey to 400 enterprises and 400 consumers around the world.

Enterprises

400 IT, Information Security and DevOps senior and C-level managers from enterprises with 1,000 or more employees were surveyed. Responses were global: Figure A (see p. 5)

Consumers

We surveyed 400 global consumers (same regions) across a wide range of ages, genders, political orientations and economic statuses: Figure B (see p. 5)



“99% of enterprise employees would consider switching vendors if they lost digital trust.”

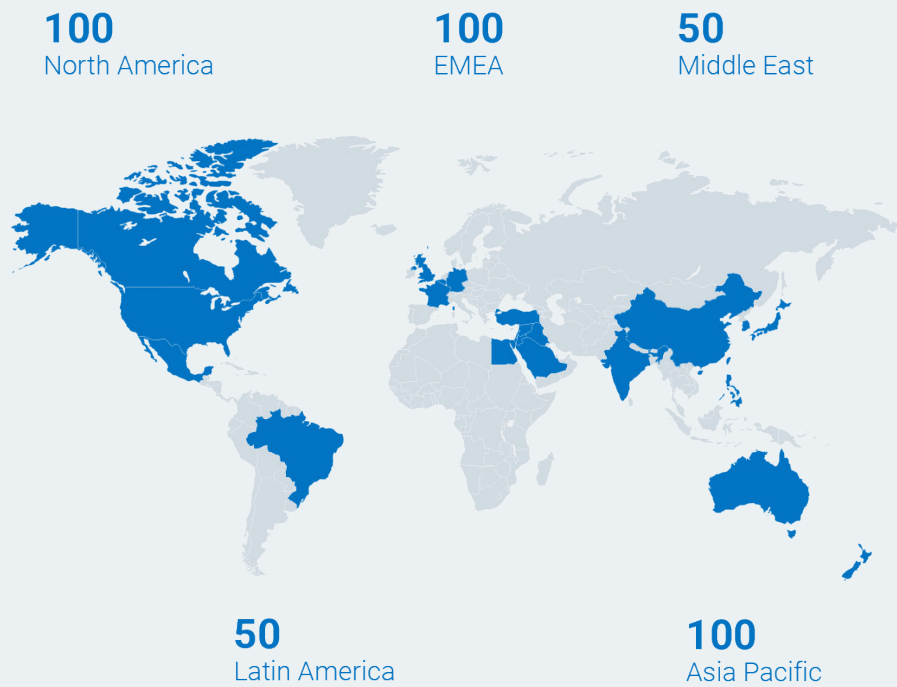


Figure A.

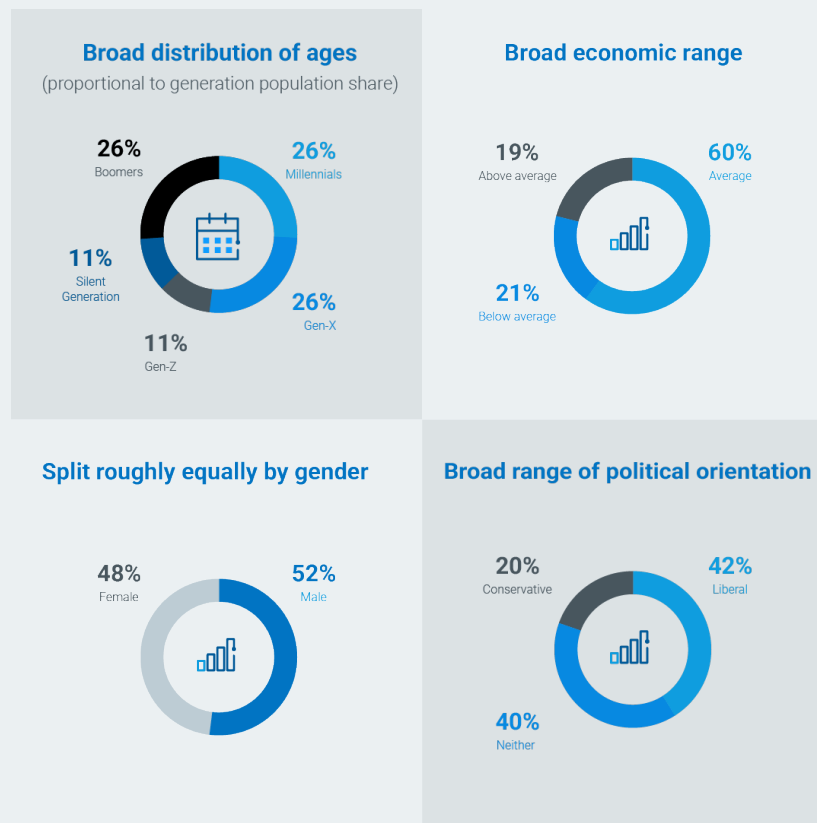
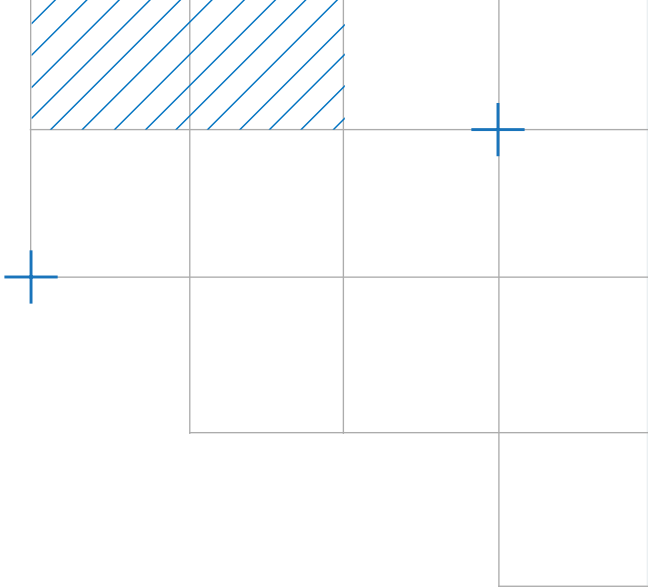


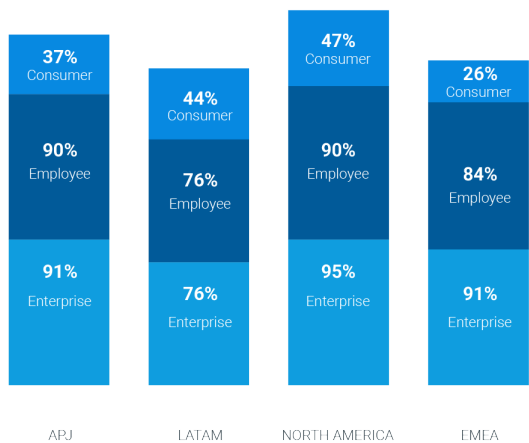
Figure B.

THE IMPORTANCE OF DIGITAL TRUST VARIES

Enterprises, employees and consumers agree that digital trust is important, but how important depends on a variety of attributes.

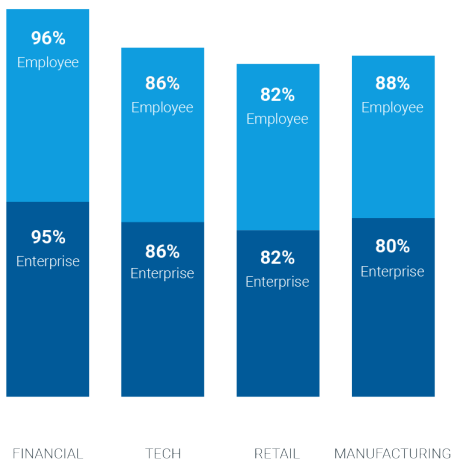


DIGITAL TRUST AS EXTREMELY IMPORTANT BY REGION



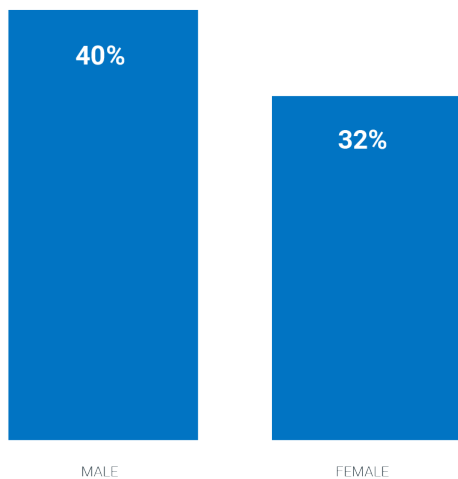
For enterprises and employees, Latin America lags in terms of feeling digital trust is extremely important. For consumers, APJ and EMEA lag. That 26% of EMEA consumers say digital trust is extremely important was surprising, given the strict EU GDPR laws enacted in 2018.

DIGITAL TRUST AS EXTREMELY IMPORTANT BY INDUSTRY



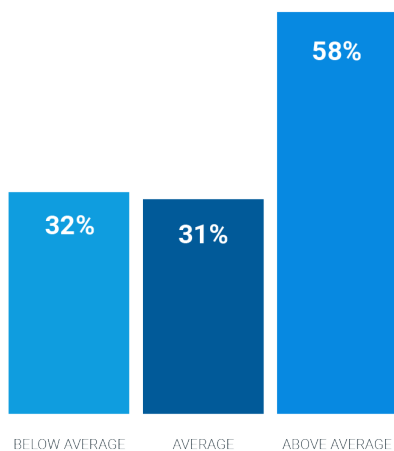
Not surprisingly, financial firms are the most likely to say digital trust is extremely important.

DIGITAL TRUST AS EXTREMELY IMPORTANT BY GENDER (CONSUMERS)



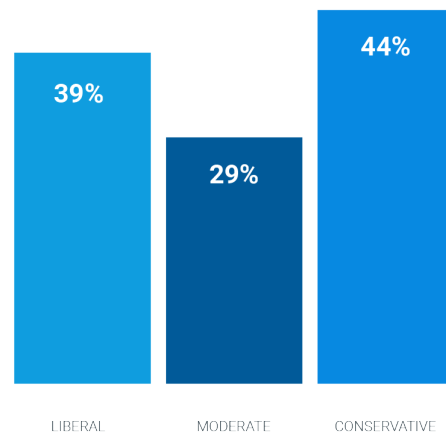
For consumers, digital trust is more important for males than females.

DIGITAL TRUST AS EXTREMELY IMPORTANT BY INCOME (CONSUMERS)



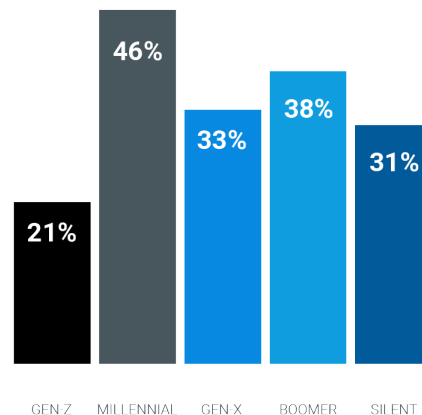
Also, digital trust matters far more to consumers with above average income.

DIGITAL TRUST AS EXTREMELY IMPORTANT BY POLITICAL AFFILIATION (CONSUMERS)



Finally, something that liberals and conservatives can agree on! Both are more likely to say digital trust is extremely important.

DIGITAL TRUST AS EXTREMELY IMPORTANT BY GENERATION (CONSUMERS)



Interestingly, the two youngest generations (and the only digital natives) are the least and the most likely to say digital trust is extremely important.

WHAT IS DRIVING THE INTEREST IN DIGITAL TRUST?

There is universal interest in digital trust, but why? What is driving this interest? We found a wide range of factors.

Growing Importance of Data. According to respondents, this was the top driver. Why? Because data is growing at a compounded rate of 23%². To put it another way, it took 70 years for the world to amass 97 Zettabytes of data at the end of 2021. By 2025, just four years later, the world will almost double that (174 ZB). That's more than 20,000 gigabytes for every person on Earth by 2025!

It isn't just the amount of data, however, but how important this data is. The data contains troves of personally identifiable information, such as what we buy, the sites we visit, our health records, social media, photographs and so much more.

Increasing Threat Surface. The enterprise has transformed its relatively static networks of data centers, offices and remote sites into far more complex hybrid networks. These new networks connect data centers, offices and remote sites, while adding thousands of work-from-home sites, multiple clouds, digital devices, edge networks and IoT devices.

In this new edgeless network, there are orders of magnitude more attack points.

Customer Expectations. As we saw in the last section, 100% of businesses and 68% of consumers rate digital trust as important. Each are likely to switch to a competitor if they lost trust in an enterprise. Digital trust has become an existential asset.

Increase in Bad Actors. The number of bad actors grows each year. These include:

- Black hat hackers
- Cyber criminals
- Cyberterrorists
- Hacktivists
- Inside actors
- Nation-state actors
- Thrill seekers and trolls

Evidence of the growth of bad actors can be seen by the record number of complaints the IC3 received in 2021: 847,376 reported complaints, which was a 7% increase from 2020³.



²Big Growth Forecasted for Big Data - IDC

³FBI Internet Crime Complaint Center (IC3)

WHAT IS AT STAKE?

What are enterprises protecting?
100% of enterprise respondents cite customer loyalty as important. This makes sense when you consider how likely customers are to switch to a competitor if they lose trust in a company.

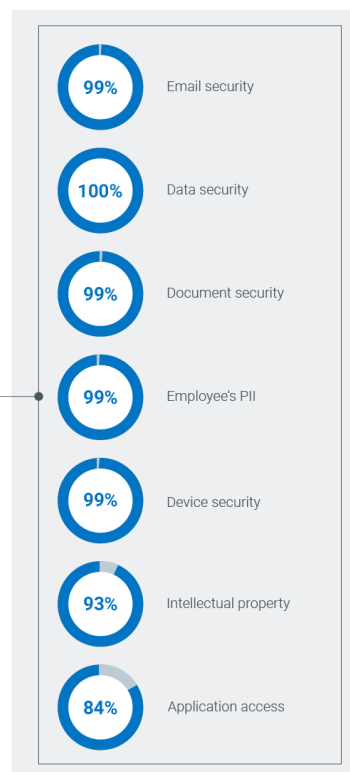
Respondents told us the types of attacks they fear most are (in order):

FOR ENTERPRISES...



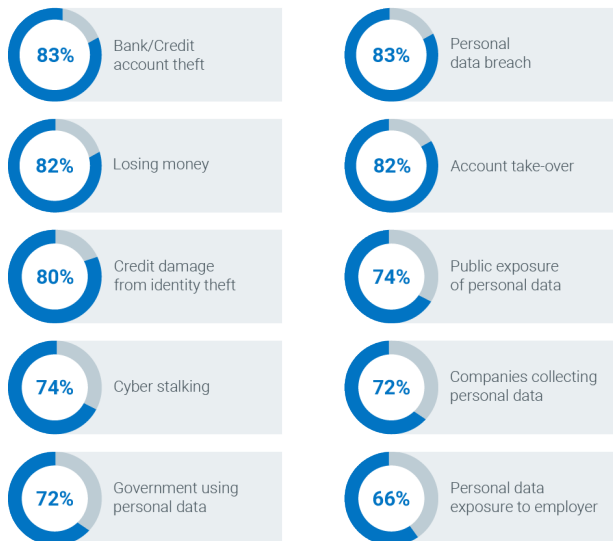
Enterprise employees have a different concern: Their personal information.

FOR EMPLOYEES...

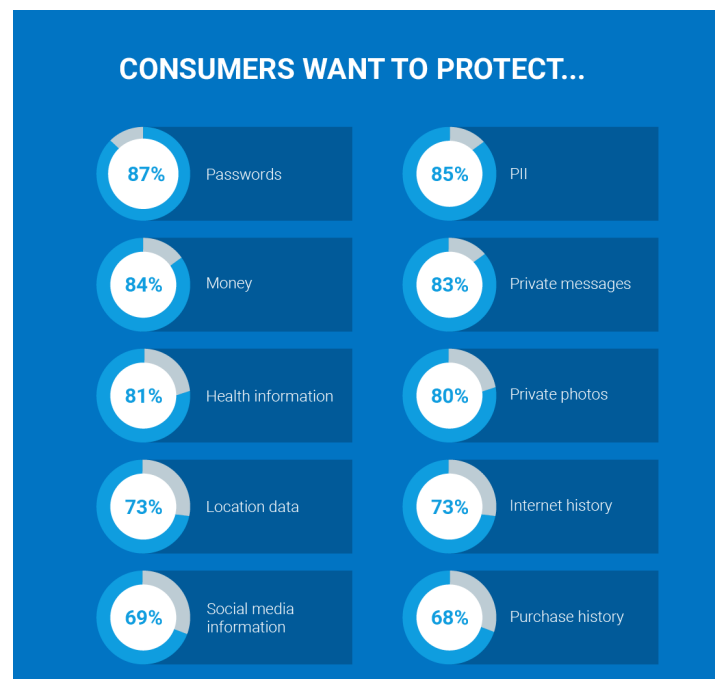


And, finally, consumers have a wide range of concerns:

CONSUMERS FEAR THESE ATTACKS...



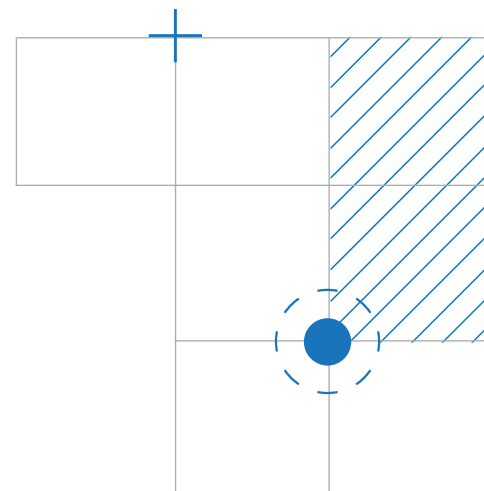
CONSUMERS WANT TO PROTECT...



We wondered whether enterprises were on the same page as consumers in terms of helping protect what matters most to consumers (passwords, personal identifiable information (PII), etc.). Virtually all attacks that compromise consumer data start with email attacks⁴. Yet, with all that enterprises do to protect consumers, they rated protecting against phishing attacks as second from the bottom in terms of how they are doing. Furthermore, they rated phishing as the attack they are most concerned about.

So, while enterprises are focused on what matters most to consumers, they have a ways to go to achieve the level of security consumers would like to see.

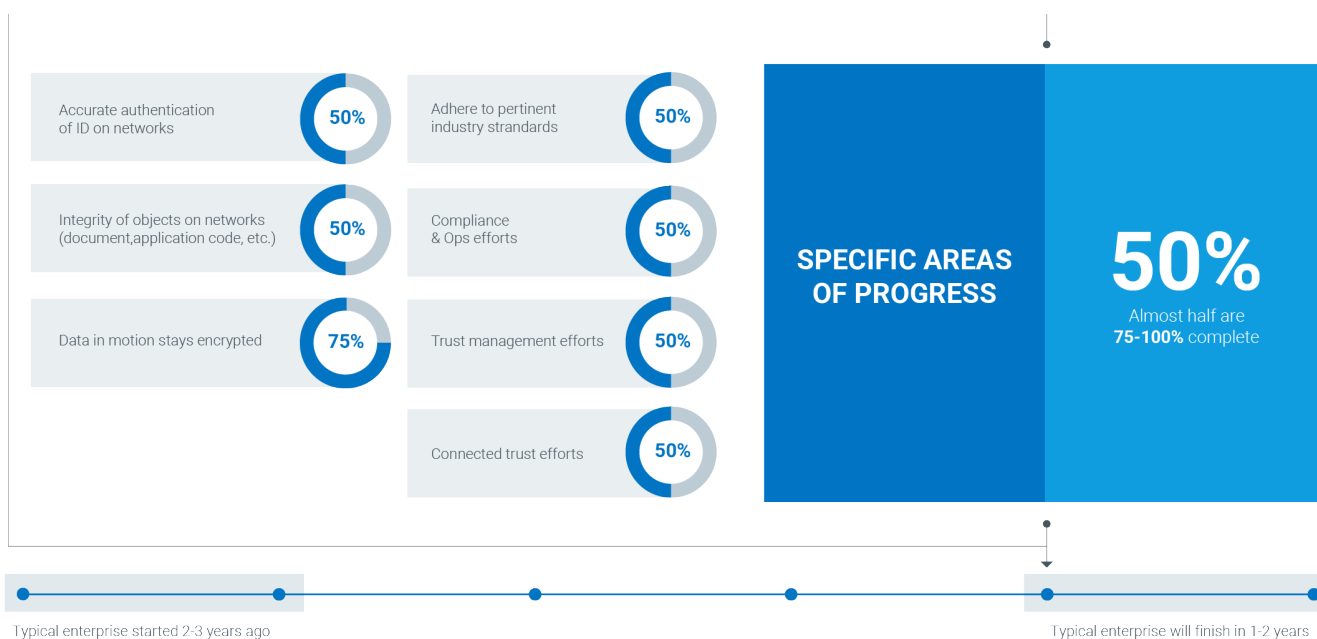
⁴Why Your Business Needs Better Email Security - Guardian Digital



HOW ARE ENTERPRISES OPTIMIZING DIGITAL TRUST?

Enterprises are engaged with digital trust. The typical organization began working on digital trust two to three years ago and has completed 75% (or more) of the journey so far. The typical organization will complete its digital trust journey in the next one to two years.

There are many facets to digital trust. We dove down further to see where enterprises were further along.



Digital Trust Goals: Enterprises clearly stated that their top goal for digital trust is customer loyalty. 100% rated this goal as important, making it the enterprises' top goal. But there were other goals as well.



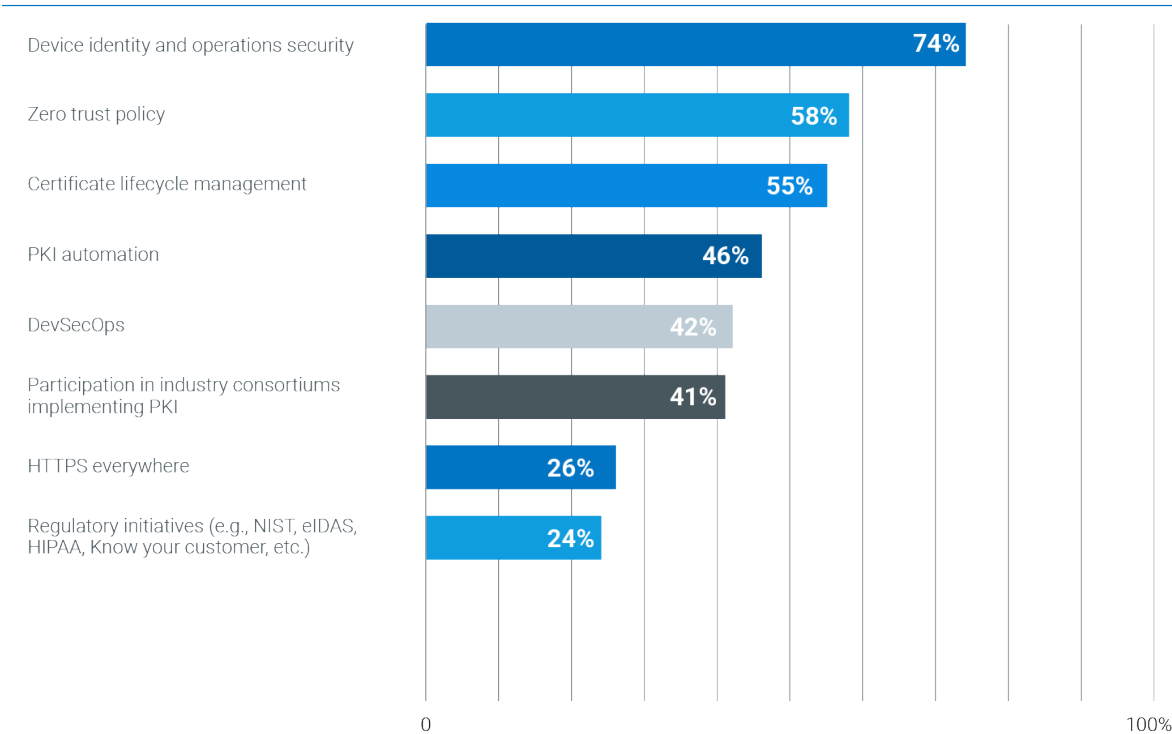
Digital Trust Challenges: Enterprises are well along in their digital trust journey, but it hasn't been easy. The number one challenge IT cited was managing digital certificates, rated as important by 100% of enterprises. Regulatory compliance and handling the massive scope of what they are protecting was a close second, at 99%. Rounding out the challenges are complexity – securing a complex dynamic, multi-vendor network – and a lack of staff expertise.

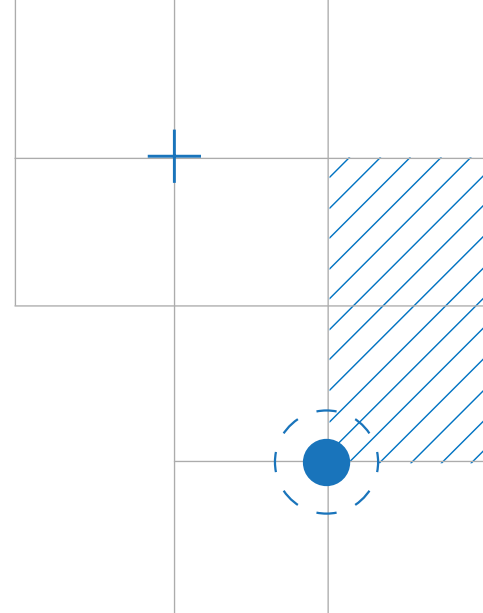


Digital Trust Practices: A wide range of initiatives can affect an enterprise's digital trust. Most enterprises are at least somewhat involved in these initiatives, but it is helpful to see which initiatives enterprises have already fully implemented.

At the top is device identity and operations security, now fully implemented now by 74% of enterprises. Zero trust policies are next in line but they are only fully implemented by 58% of enterprises. The only other initiative implemented by more than half of enterprises (55%) is certificate lifecycle management Rounding out the list were:

Q22: What is your involvement with the following Digital Trust practices?
(Already implemented)



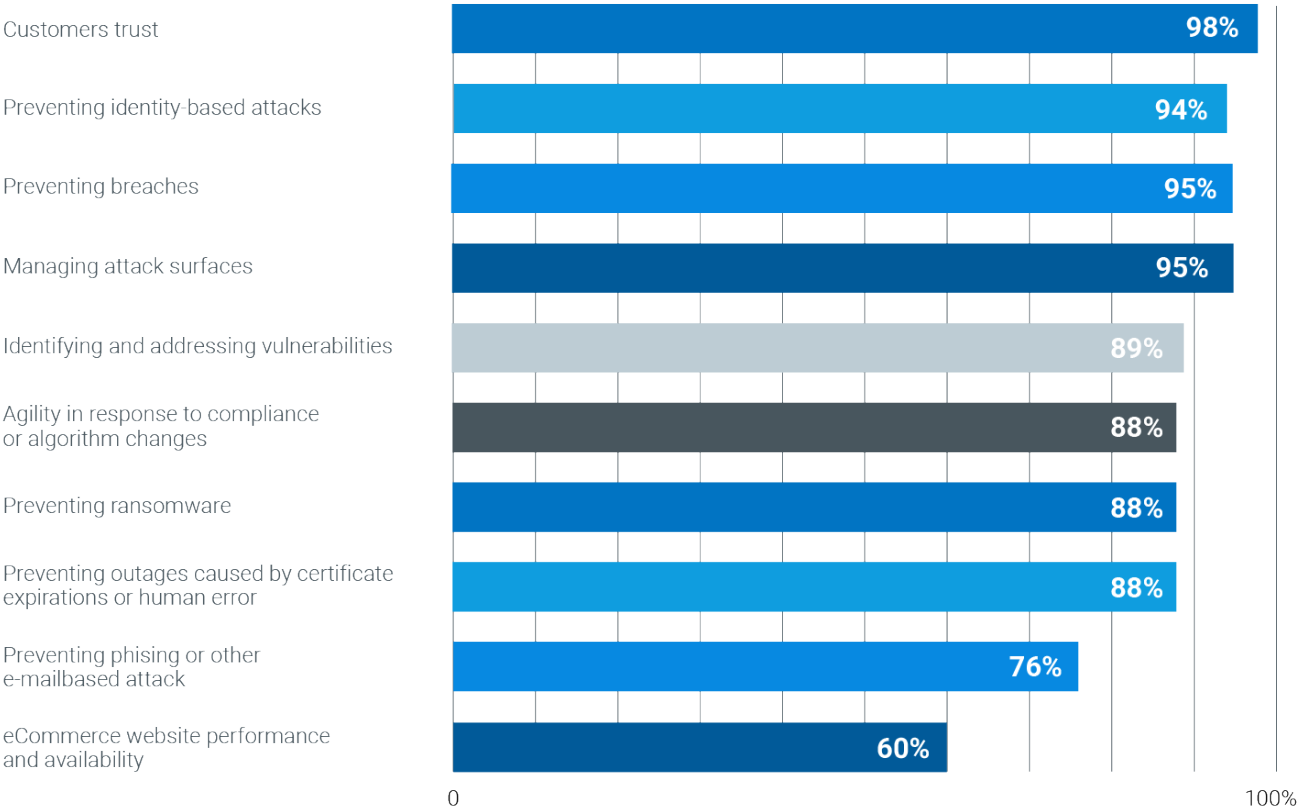


HOW ARE ENTERPRISES DOING WITH DIGITAL TRUST METRICS?

Enterprises are doing quite well across a broad set of digital trust goal metrics. Take their top goal (customer trust) for example. 98% are doing well with this goal (with 61% doing extremely well). They are also doing well with preventing breaches (95%, with 51% doing extremely well) and identity-based attacks (94%, with 50% doing extremely well).

In fact, in eight of ten of the metrics we studied, at least seven of eight enterprises said they were doing well. It was only preventing phishing or other email-based attacks and eCommerce website performance and availability that fell behind (76% and 60% respectively).

Q23: How well are you doing with each of the following Digital Trust metrics?
(Somewhat/Extremely Well)



Customers are Seeing Improvement

All (100%) enterprises report that digital trust is important to their customers, with 91% saying their customers rate digital trust as extremely important.

So it's essential to take stock of how customers perceive their digital trust. From the enterprises' perspective, the news is good, with 99% of enterprises saying their customers have more confidence in the enterprise's digital trust today than in the past. Nearly three quarters (73%) say it is significantly more.

So how do businesses feel? Do they share this optimism? In fact, the numbers are almost identical. When asked to rate the confidence enterprises have in the businesses they interact with, 98% say there is more today than in the past, and 76% say there is extremely more.

But that's for B2B interactions. What about B2C? Here the numbers are not as optimistic as with B2B. Less than half say their digital trust in the organizations they deal with is more than in the past, while 54% say there is room for improvement.



"91% of customers rate digital trust as extremely important."

North American Results

North America (U.S. and Canada) leads the world in terms of rating digital trust as extremely important. This is true for enterprises, employees and consumers.

Notably, North American consumers are the most concerned about cyber-threats (like bank accounts or credit cards being accessed and money stolen) than consumers anywhere else in the world other than Asia Pacific. (91% of APAC consumers are concerned about these threats versus 85% for

North America and 77% and 78% in EMEA and LATAM, respectively.)

All of this shows in the high score consumers give North American enterprises. In terms of digital trust success, 31% of North American consumers say they have significantly more trust in the companies they do business with. APAC consumers are in the middle with 19%. This compares to 24% for Latin American consumers and just 19% and 15% for APAC and EMEA consumers, respectively.

APAC Results

Across the board, Asia-Pacific sees digital trust as extremely important. They are more focused on digital trust than any other region besides North America.

In part, this is because APAC consumers are the more concerned about cyber-threats (like bank accounts or credit cards being accessed and money stolen) than consumers anywhere else in the world. (91% of APAC consumers are concerned

about these threats, versus 85% for North America and 77% and 78% in EMEA and LATAM, respectively.)

In terms of digital trust success, APAC consumers are in the middle, with 19% saying they have significantly more trust in the companies they do business with. North America and Latin American consumers report 31% and 24% respectively, whereas EMEA consumers report just 15%.

LATAM Results

Across the board, Latin America lags behind the world in terms of seeing digital trust as extremely important.

This is partly because Latin American consumers are less concerned about cyber-threats (like bank accounts or credit cards being accessed and money stolen) than most consumers. (Just 78% of LATAM consumers are concerned about these threats, versus 91% of APAC consumers, 85% of

North American and 77% of EMEA consumers.)

In terms of digital trust, LATAM consumers report relatively high success, with 24% of LATAM consumers saying they have significantly more trust in the companies they do business with. By comparison, North American consumers reported 31% and APAC and EMEA consumers reported 19% and 15%, respectively.

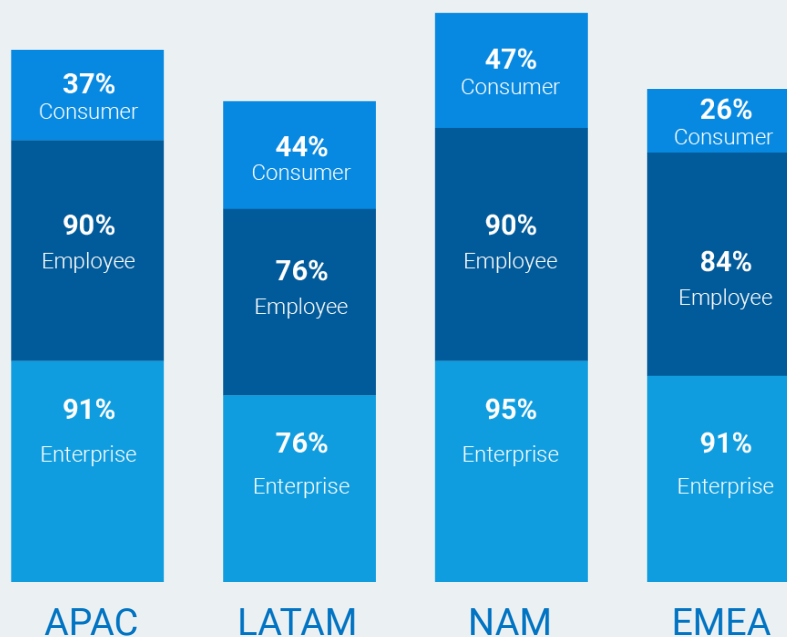
EMEA Results

For a region with some of the most stringent privacy laws (GDPR), EMEA consumers are surprisingly blasé about digital trust. Overall, EMEA ranks 3rd in terms of how they rate the importance of digital trust. But if you dig into the data, EMEA has a strong interest at the enterprise level, and a medium interest at the employee level. It is the consumer level where we see digital trust importance numbers at almost half of North America's.

This correlates with the concern about cyber-threats. EMEA consumers have the lowest level of concern for cyber-threats like bank accounts or credit cards being accessed and money stolen. Just 77% of EMEA consumers are concerned about these threats, compared to 78% of LATAM, 85% for North America and 91% of APAC consumers.

This also correlates with the relatively low percentage of EMEA consumers who say their trust of the companies they do business with has increased in recent years (just 15%). This lags behind APAC (19%), LATAM (24%) and North America (31%).

DIGITAL TRUST AS EXTREMELY IMPORTANT BY REGION



LESSONS FROM THE DIGITAL TRUST COGNOSCENTI

As seen in the last section, enterprises seem to be doing quite well in their digital trust efforts. We wanted to see if this was universally true, or if there were groups of enterprises that did significantly better or worse than average.

To explore this, we scored their answers to the metric questions:

Scoring Guide

- Extremely poorly -2
- Somewhat poorly -1
- Neither poorly nor well 0
- Somewhat well +1
- Extremely well +2

We then added three individual scores to create a total score for each respondent. We divided the respondents into three tiers:

Enterprise Digital Trust Tiers

- Top tier (scores were in the top third of all respondents)
- Middle tier (middle third)
- Bottom tier (lowest third)

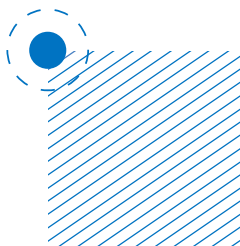
This tiering exposed some dramatic differences between the very best enterprises (the top tier) and the very worst (the bottom tier).

How Much Better?

It is axiomatic that the top tier is doing better with the digital trust metrics, since that is how we divided the respondents into tiers in the first place. But what's interesting is just how much better the top tier is doing than the bottom tier. For example, three times as many top-tier enterprises report doing well with eCommerce website performance and availability, and 2.9 times as many say they're doing well at preventing phishing or other email-based attacks. The top tier ranges from 10% better to 300% better in every metric:

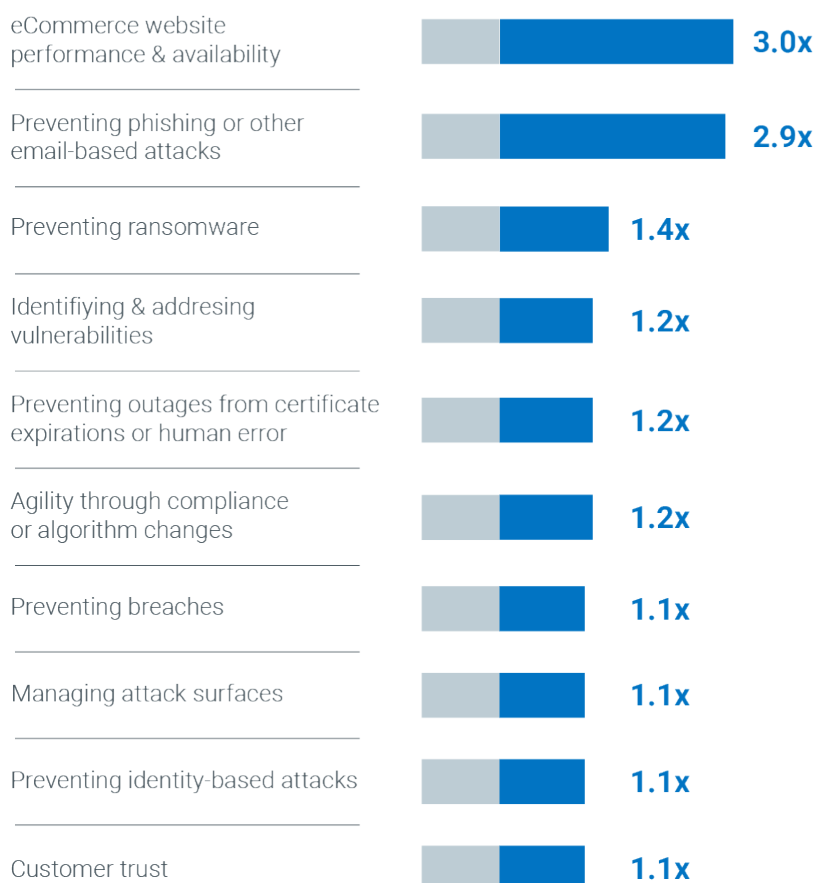


TOP-TIER ORGANIZATIONS' CUSTOMERS ARE SIGNIFICANTLY MORE LIKELY TO TRUST THEM THAN ARE THE CUSTOMERS OF THE **BOTTOM TIER**.



²Big Growth Forecasted for Big Data - IDC
³FBI Internet Crime Complaint Center (IC3)

THE BEST ENTERPRISES ARE DOING **MUCH** BETTER WITH DIGITAL TRUST THAN THE WORST

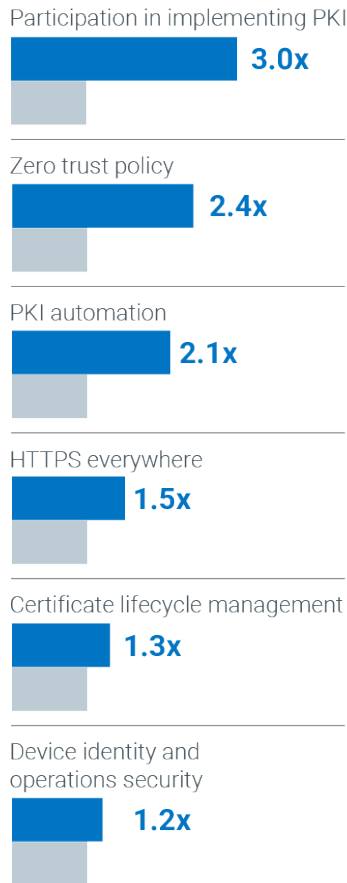


Why is the Top Tier Doing So Much Better?

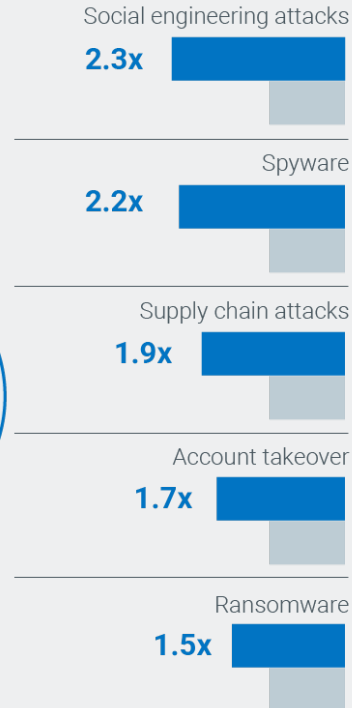
There are a variety of striking differences between the top tier and bottom tier that are driving these big differences in digital trust outcomes:

- **Attitudes:** The top tier is four and a half times as likely to believe a loss of customer trust will lead to a loss of that customer. They are also more likely to believe that digital trust affects their brand, sales and margin. In addition, they are also 5.6 times as likely to say they would switch partners if they lost trust in that partner.
- **Earlier Start:** The top tier is further along in their digital trust journey and will complete that journey much earlier than the bottom tier.
- **More Concerned about Cyber Threats:** The top tier takes cyber threats much more seriously. The top tier is 1.5 to 2.3 times as likely to be concerned about cyber threats.
- **More Engaged with Common Cyber Safeguards:** The top tier is up to three times as likely to be engaged with important cyber-security safeguards.

HOW MUCH **MORE** LIKELY ARE THE **TOP TIER** TO BE ENGAGED WITH:



TOP TIER IS **MORE** CONCERNED ABOUT SOME IMPORTANT CYBER THREATS:



Where Should Digital Trust Reside?

Deciding where digital trust is placed in an enterprise organization is an important decision. There is a clear difference of opinion on this issue between the top- and bottom-tier enterprises.

The top tier overwhelmingly says that the CIO should run digital trust in the IT organization, whereas the bottom tier disagrees, feeling that security operations should run it.

This is not a slight on security operations or its role, which is vital to an organization. It should be viewed as an acknowledgment of the CIO's visibility into the broader technology footprint of an organization and how important digital trust is to a technology-driven organization's success. This finding reflects the top tier enterprises' strategic approach to digital trust.

DIGICERT'S TAKE

DigiCert, the leading global provider of digital trust, which enables individuals and businesses to engage online with the confidence that their footprint in the digital world is secure has been involved in digital trust from the earliest days. Our advice for companies wishing to emulate the success demonstrated by the top-tier “Digital Trust Cognoscenti” is to consider doing the following five things:



Make digital trust a strategic imperative. This was one of the clear differentiators for the top-tier enterprises, which recognized that digital trust affects important business outcomes such as brand, customer loyalty, revenue and margins.



Establish a Digital Trust Office within your organization's technology function with a clear leader empowered with decision-making power.



Recognize that digital trust awareness is rising among your users, including consumers, and that your business success and reputation are tied directly to your ability to ensure digital trust at a high level.

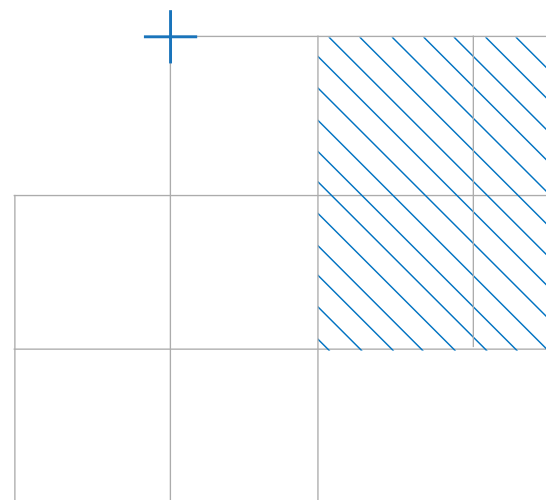


Enlist expert help in your quest for digital trust. One of the digital trust challenges cited by enterprises was a lack of staff expertise. Make sure the partners you bring on have a comprehensive portfolio spanning the building blocks of digital trust and can provide solutions for unified trust management for your entire organization.

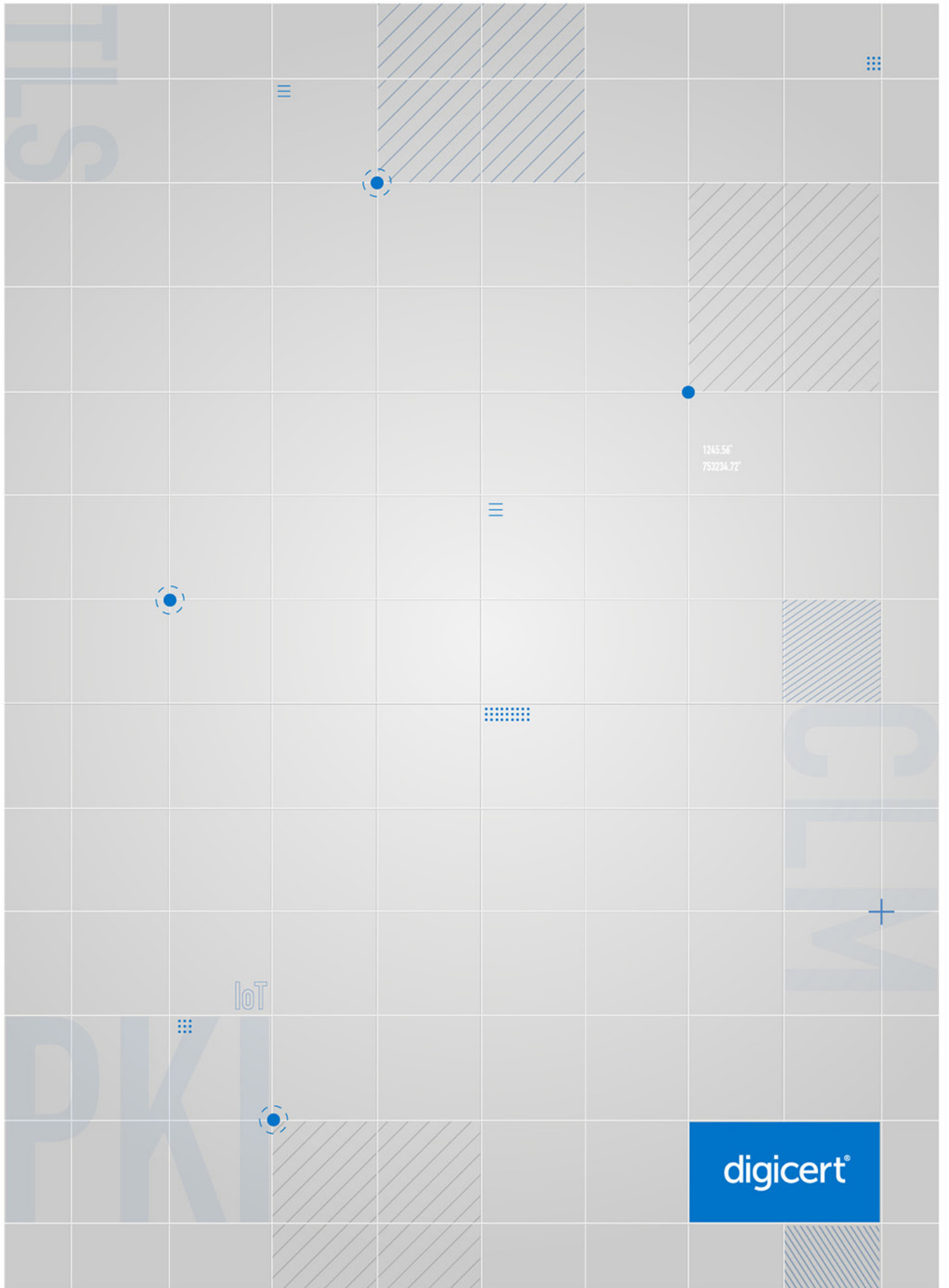


Remember — your customers care about digital trust. Establish clear lines of digital trust communication with them, explaining not only your commitment to digital trust but also your progress.

This falls in line with a notable study by Bain & Company⁵ which found that increasing customer retention rates by 5% increases profits by 25% to 95%. Given how likely customers are to leave a company if they lose trust in them, maximizing digital trust should be a mandatory activity.



⁵Prescription for Cutting Costs – Bain & Company



digicert®