Guardians of Trust

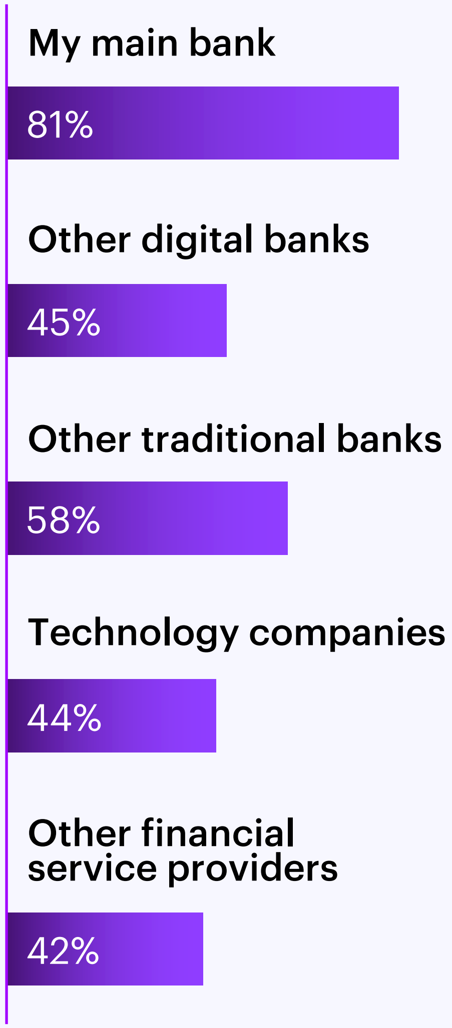
Navigating Cybersecurity in Banking

While consumers trust their banks' ability to protect their personal and financial data, they have less trust in the banks' third parties and the broader banking system.

58%

of banking customers are concerned about the security of their personal and financial data and the potential to be hacked.*

How much do you trust your bank to keep your personal data secure?



Source:
Accenture "Banking Consumer Study 2025"

*Accenture "Banking Consumer Study 2025"

And consumers are on to something…

According to the World Economic Forum Global Cybersecurity Outlook 2025*, supply chain vulnerabilities are emerging as the top ecosystem cybersecurity risk.

As a matter of fact, according Accenture's Guardians of Trust survey, 54% of banks experienced material impacts from a cyber incident caused by a third party in the last year*.

This concern over trust is a growing challenge for banks as they expand their reliance on third parties, and particularly as they accelerate their adoption of AI.

56%

projected growth in banking sectors' spending on gen AI over the next 4 years. Moreover, 86% of bank executives say gen AI is a key driver to improve customer experience.

* Global Cybersecurity Outlook 2025

* All the data is coming from Accenture "Guardians of Trust. Navigating the cybersecurity in banking" survey unless stated otherwise.

However, banks are challenged with keeping up with securing gen AI and protecting the banks and their customers against gen AI powered threats.

83%

of banks report challenges in aligning security measures that the pace they adopt new technologies like gen AI.

Only

12%

of banks believe that balancing customer demands for seamless and frictionless experiences across all platforms without compromising security is not challenging.

Only

32%

of banks agree they embed security controls in all transformation initiatives by design.

And threat actors are also taking advantage of gen AI capabilities to increasingly target banks, third parties, and consumers.

AI powered attacks on banks were ranked as the #1 activity in the past 12 months.

Managing cybersecurity and communicating transparently about cybersecurity practices critical to banks' customer retention.

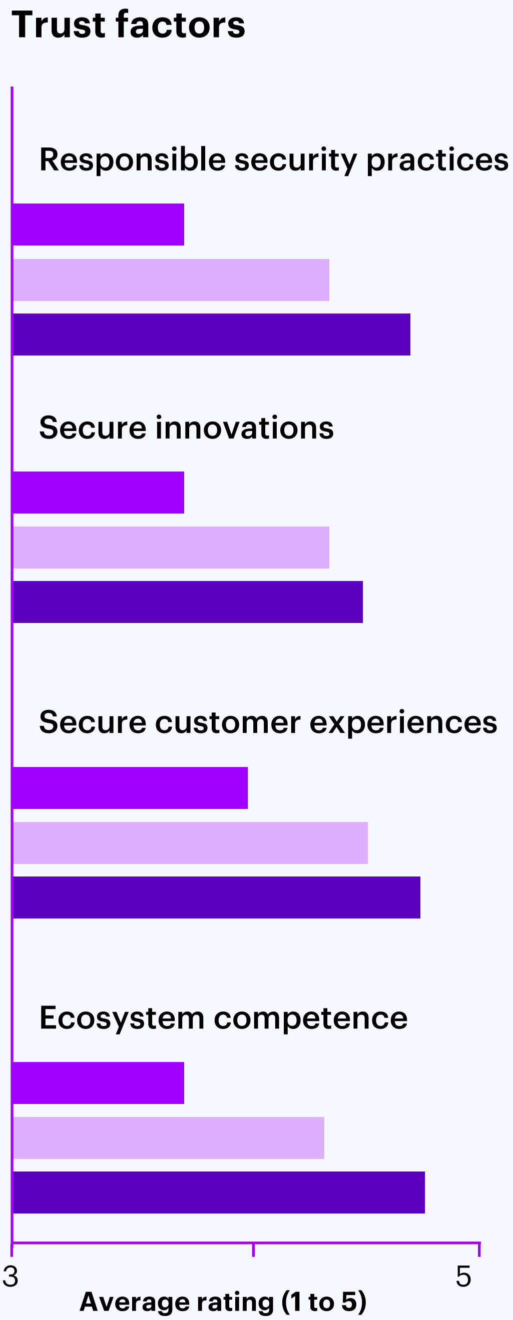
85%

of banking customers say clear communication about cybersecurity practices is essential.

However there is a gap in how banks perceive their efforts versus how consumers view their trust in their banks' cybersecurity and banks need to take action to close this gap or risk consequences to their business.

● Consumer confidence
● Banks' perception
● Importance to customers

How consumers and banks view trust across key factors?



Managing cybersecurity and communicating transparently about cybersecurity practices critical to banks' customer retention.

91%

of customers rate data security, fraud protection, and privacy as must-haves.

62%

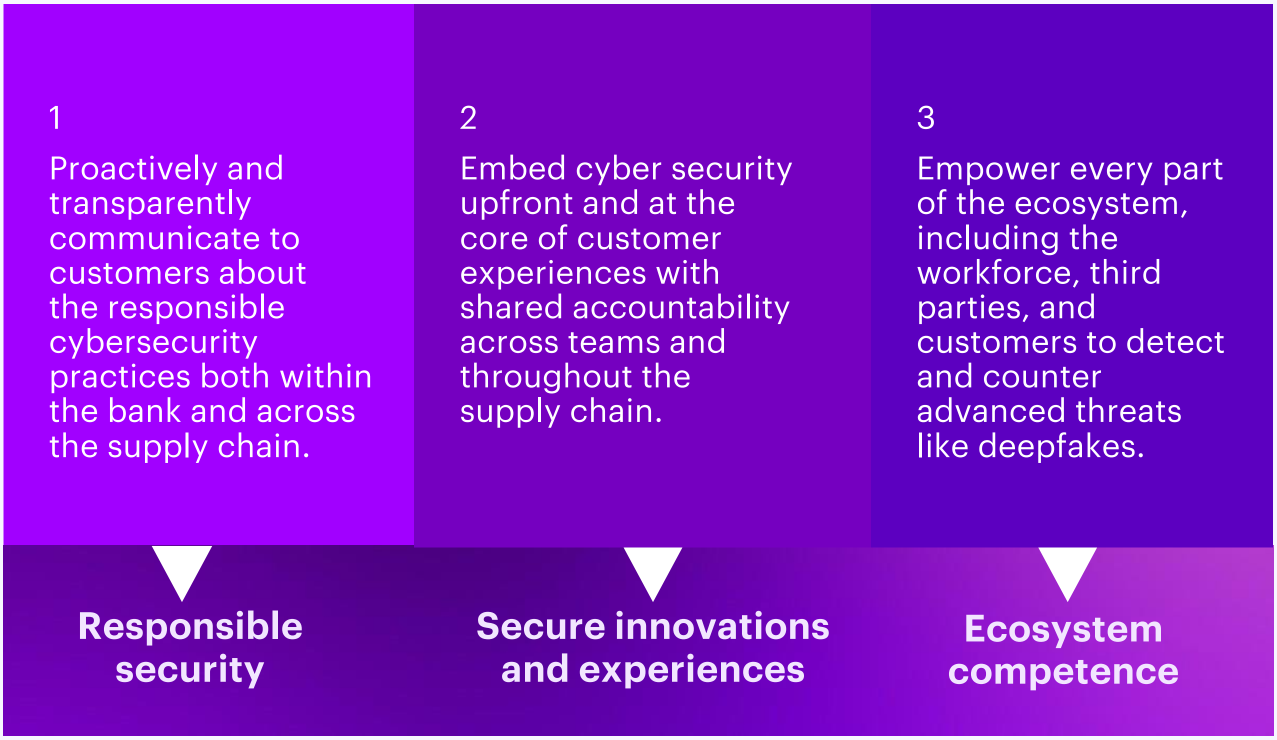
of customers lose trust in their banks' brand following a data breach

43%

of consumers will stop engaging with their bank following a data breach

1 in 2 bank executives that witnessed in increase in data breaches also reported an increase in customer attrition

Our research identified 58 practices used by the top 10% of banks that have strong customer trust (called “Guardians of Trust”). These practices are divided into three categories: Responsible security, Secure innovations and experiences and Ecosystem competence and help the leading banks build and maintain trust despite increasing cyber risks.



1

Proactively and transparently communicate to customers about the responsible cybersecurity practices both within the bank and across the supply chain.

Responsible security

2

Embed cyber security upfront and at the core of customer experiences with shared accountability across teams and throughout the supply chain.

Secure innovations and experiences

3

Empower every part of the ecosystem, including the workforce, third parties, and customers to detect and counter advanced threats like deepfakes.

Ecosystem competence

1

Proactively and transparently communicate responsible cybersecurity practices to customers.

Guardians of Trust show a 41-point higher commitment to responsible cybersecurity practices than their lagging peers on the trust index (Figure 1). This success stems from three core actions essential for navigating emerging threats, meeting regulatory requirements and building lasting customer trust.

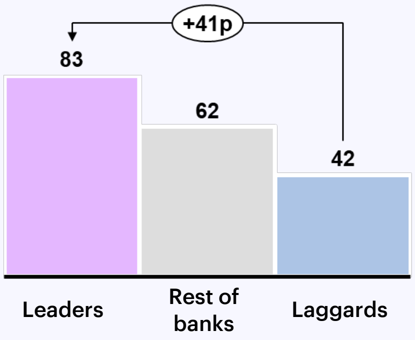


Figure 1

Trust Index Score: Responsible Security

Actions to take:

Build customer trust with transparent communication of cybersecurity practices

Proactively strengthen governance, risk management and compliance with automation and AI

Establish a responsible and secure AI framework

2

Embed cyber security upfront and at the core of customer experiences with shared accountability across teams and throughout the supply chain.

As banks adopt advanced technologies like generative AI and digital platforms, embedding cybersecurity and operational resilience from the start is essential to deliver seamless and safe customer experiences. Security should be integrated at every customer touchpoint, with shared accountability across technology, security and business teams.

Guardians of Trust excel in this area, outperforming their peers by 38 points in the secure innovations and experiences pillar of the trust index (Figure 2). Nearly all top performers (98%) embed cybersecurity by design, investing 58% more in 2024 than laggards, with plans to increase technology budgets by 1.3 times over the next three years.

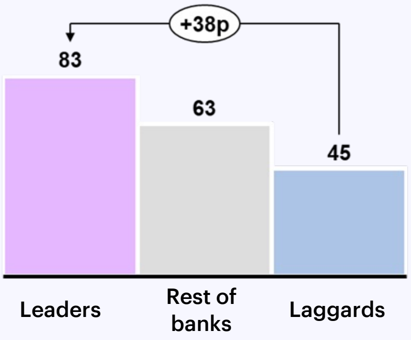


Figure 2

Trust Index Score: Secure Innovations and Experiences

Actions to take:

Align cybersecurity with broader organizational goals and establish shared accountability across the C-suite

Partner closely with technology and business teams to integrate security into business practices, enhancing customer acquisition and retention

Modernize and scale digital core security with gen AI and cybersecurity as a service (CaaS) for resilient cyber defense

Strengthen Open Banking APIs with robust security and third-party risk management

Implement seamless adaptive authentication and AI-driven risk management to secure digital trust

3

Empower every part of the ecosystem, including the workforce, third parties and customers to detect and counter advanced threats like deepfakes.

Guardians of Trust place 39 points more emphasis on workforce security training and education than their lagging counterparts, underscoring its importance in maintaining customer trust (Figure 3). Notably, 98% of these banks demonstrate a strong understanding of the evolving cybersecurity threat landscape. Furthermore, all confirmed that their employees are not only well-versed in cybersecurity but also consistently apply best practices.

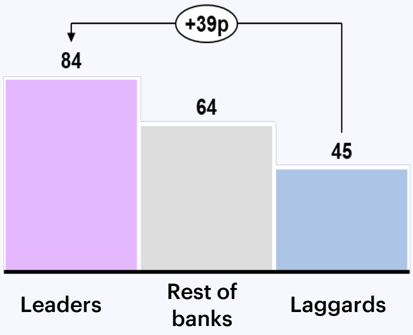


Figure 3

Trust Index Score: Workforce Competence

Actions to take:

Enhance ecosystem competencies through training and education

Foster a culture of collaboration and recognition

Supercharge threat detection and response with AI and automation

We found that Guardians of Trust, who prioritize these trust practices demonstrate superior results across key performance measures.

Performance indicators – Leaders vs laggards (bottom 25%)

Security

Identify/ Detect threats saster

2.3X more likely to detect threats in less than 10 days in comparison to laggards

Contain threats faster

2.5X more likely to contain threats in less than 1 day in comparison to laggards

Remediate faster

2.3X more likely to remediate threats in less than 20 days in comparison to laggards

Stronger security posture

144% less cyber attack attempts than laggards (over the past 3 years)

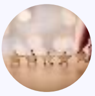
58% less data breaches than laggards (over the past 3 years)

Customer* & Brand*

Customer retention

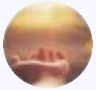
↑ **1.5X**

Customer experience



↑ **2.2X**

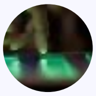
Brand reputation



↑ **2.6X**

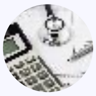
Financial*

Revenue growth



↑ **2.3X**

Cost reduction



↓ **1.7X**

Balance sheet performance/ improvements

↑ **1.7X**

*Impact of cybersecurity on financial, customer & brand performance indicators

About Research

To inform this research we conducted two surveys in October 2024: a consumer survey of more than 1400 banking consumers in 17 countries; and a banking survey of 600 banking security executives across the same 17 countries with assets above US$ 50 billion.

Countries included: Australia, Brazil, Canada, Germany, Spain, France, India, Italy, Japan, Mexico, Singapore, Saudi Arabia, South Africa, Netherlands, UAE, United Kingdom, United States.

Cybersecurity Trust Framework – Methodology

We developed a structured trust framework based on a comprehensive analysis of trust’s two core components: Character (intent, integrity) and Competence (capability) which included three phases:

1. Identified 58 best practices essential for building trust in cybersecurity by examining both the character and competence of banks. Our approach included: surveying banking consumers to understand the trust factors they value most. Through linear regression analysis, controlling for customer work type and geography, we found a strong positive correlation between the identified security practices and the level of customer trust. Additionally, conducted an extensive review of empirical literature on cybersecurity trust using AI, to validate the best practices and gathered perspectives from both internal and external subject matter experts, combined with our experience working with high-performing organizations.

2. Tested these 58 practices by evaluating a global sample of 600 banks, identifying a leading group in the top 10% that adopted these practices with significantly greater intensity. A cluster analysis revealed a strong positive association between the adoption of these practices and key performance indicators.

3. Grouped these 58 practices into three key cybersecurity trust themes and created a benchmarking asset—the Cybersecurity Trust Index—which measures and computes trust adoption scores for banks.

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent and innovation led company with 738,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology with unmatched industry experience, functional expertise and global delivery capability. We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Accenture Song. These capabilities, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients succeed and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities.

Visit us at www.accenture.com

About Accenture Research

Accenture Research creates thought leadership about the most pressing business issues organizations face. Combining innovative research techniques, such as data-science-led analysis, with a deep understanding of industry and technology, our team of

300 researchers in 20 countries publish hundreds of reports, articles and points of view every year. Our thought-provoking research developed with world leading organizations helps our clients embrace change, create value and deliver on the power of technology and human ingenuity. For more information, visit Accenture Research on www.accenture.com/research.

Disclaimer: The material in this document reflects information available at the point in time at which this document was prepared as indicated by the date in the document properties, however the global situation is rapidly evolving and the position may change. This content is provided for general information purposes only, does not take into account the reader's specific circumstances, and is not intended to be used in place of consultation with our professionaladvisors. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals. This document refers to marks owned by third parties.

All such third-party marks are the property of their respective owners. No sponsorship, endorsement or approval of this content by the owners of such marks is intended, expressed or implied.