Trust, Resilience and the Art of Keeping Your Job!

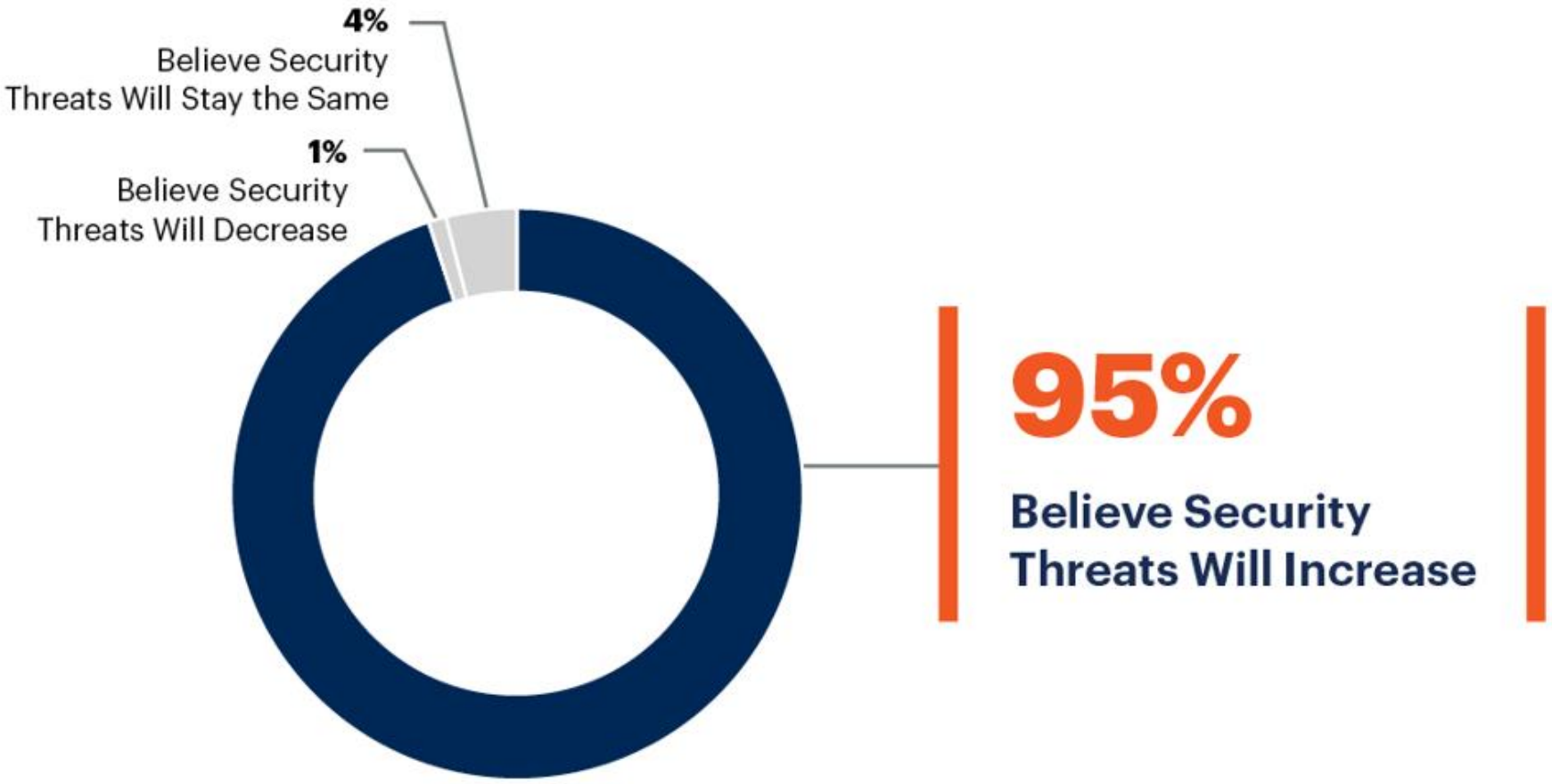
E. Mastranza
Executive Partner, Iberia

Gartner®

What's new? What's not?

Cybersecurity Threats Can’t Wait

Percentage of Respondents

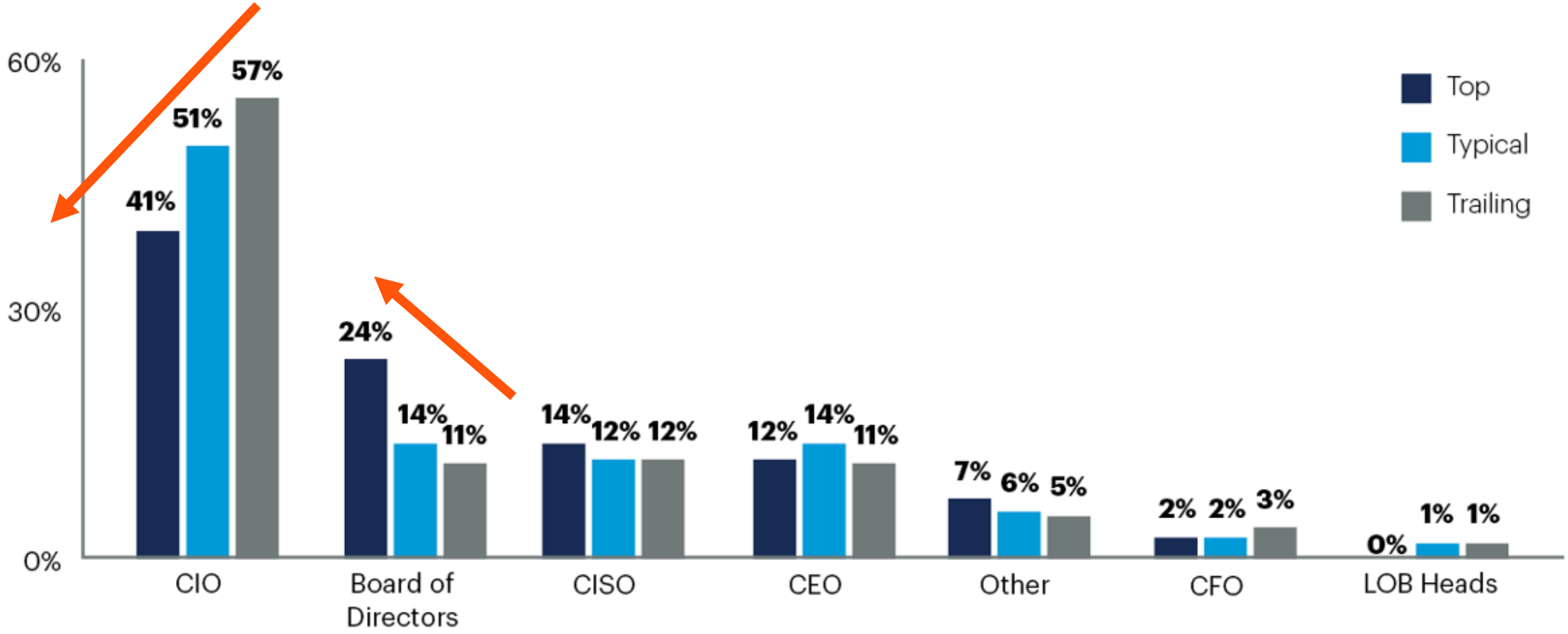


Q. In three years, do you believe cybersecurity threats will decrease, remain the same or increase?
n = 2,868.

Gartner

Responsibility for Cybersecurity

Percentage of Respondents



Q. Who is ultimately accountable for cybersecurity in your organization?
n = 228 (top performers), 2,313 (typical performers), 275 (trailing performers).
Base: All answering, excluding don't know/prefer not to answer.

Gartner

Top Priorities for 2018 and 2019

Percentage of Respondents

	Financial Services (n = 327)		Top Performers (n = 225)		Typical Performers (n = 2,244)		Trailing Performers (n = 274)	
1	Digital transformation	34%	Digital transformation	31%	Digital transformation	23%	Revenue/business growth	24%
2	Revenue/business growth	18%	Revenue/business growth	20%	Revenue/business growth	21%	Operational excellence	15%
3	Operational excellence	10%	Operational excellence	16%	Operational excellence	13%	Cost optimization/reduction	11%
4	Customer experience	10%	Customer experience	11%	Customer experience	9%	Digital transformation	10%
5	Cost optimization/reduction	9%	Data and analytics	7%	Cost optimization/reduction	8%	Business/financial goals	8%
6	Data and analytics	8%	New products/services	7%	Business/financial goals	7%	Modernization (of legacy systems)	7%
7	Modernization (of legacy systems)	7%	Cost optimization/reduction	7%	Business model change	6%	Data and analytics	7%
8	Business model change	7%	Artificial intelligence/ machine learning	6%	Industry-specific	6%	Industry-specific	7%
9	Security	6%	Business model change	6%	Data and analytics	5%	Enterprise resource planning	6%
10	New products/services	5%	Industry-specific	6%	New products/services	5%	Business model change	5%

Base: All answering, excluding prefer not to answer; n varies by segment.
Showing the 10 most common answers per segment, coded open-text responses; multiple responses allowed.
Q: What would you say is your organization's top priority for 2018 and 2019?

Gartner

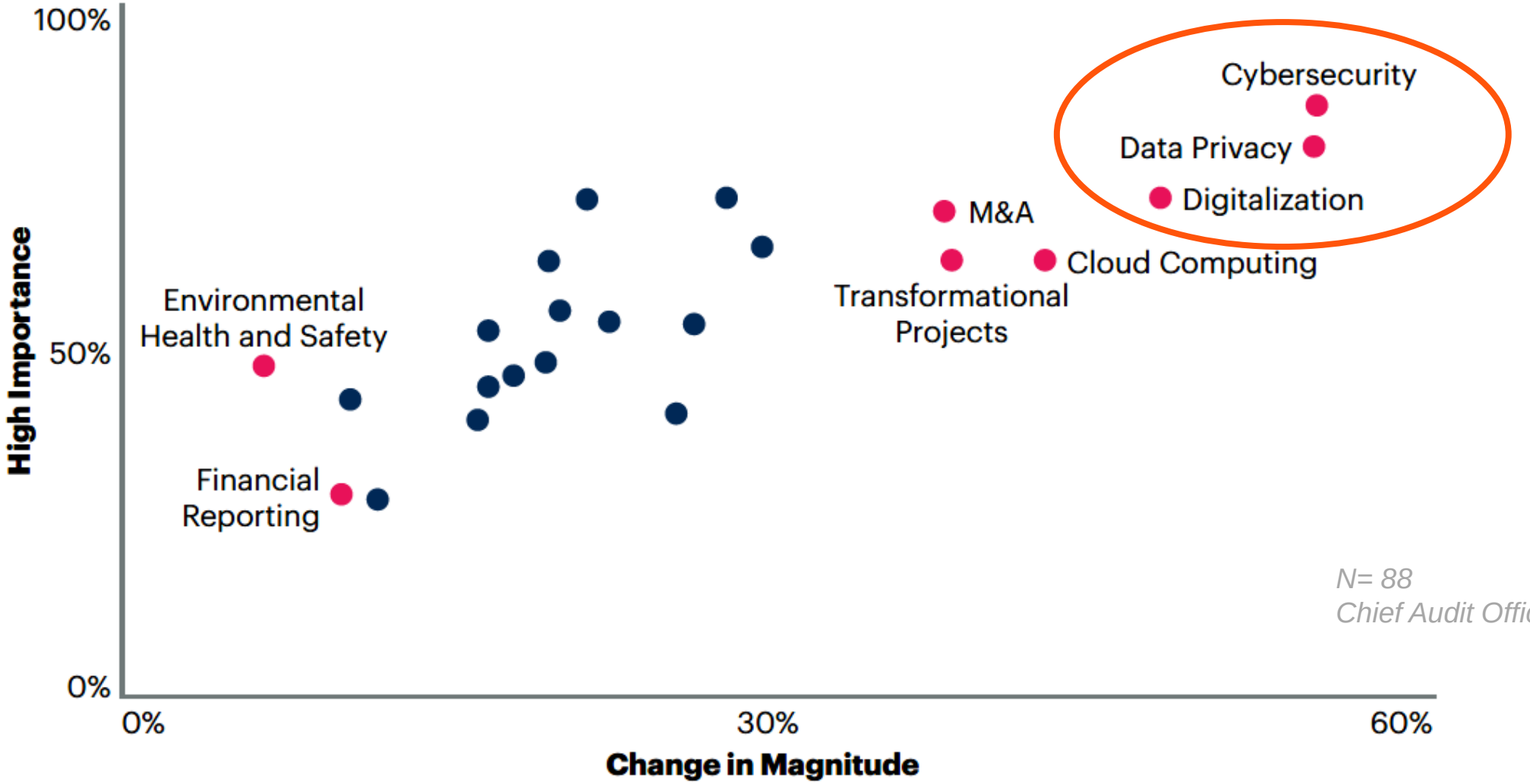
Top Technology Areas for New Spending

Percentage of Respondents

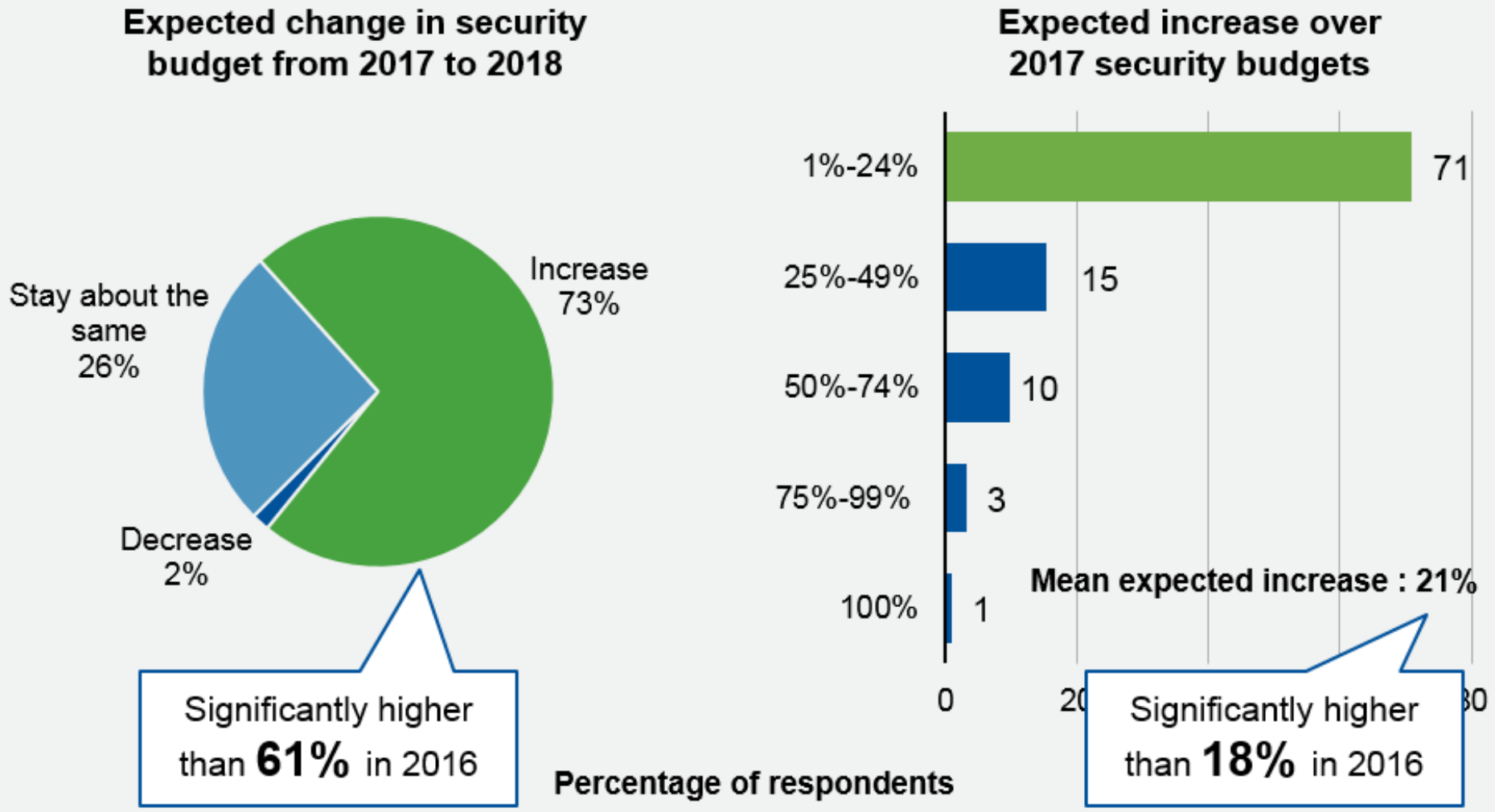
	Financial Services (n = 411)		Top Performers (n = 248)		Typical Performers (n = 2,540)		Trailing Performers (n = 298)	
1	Business intelligence/data analytics solution	46%	Artificial intelligence/machine learning	48%	Business intelligence/data analytics solution	46%	Business intelligence/data analytics solution	43%
2	Cyber/information security	44%	Business intelligence/data analytics solution	41%	Cyber/information security	40%	Cyber/information security	43%
3	Digital business initiatives	44%	Digital business initiatives	40%	Cloud services/solutions	32%	Cloud services/solutions	38%
4	Core system improvements/ transformation	37%	Customer/user experience	34%	Core system improvements/ transformation	32%	Core system improvements/ transformation	31%
5	Customer/user experience	35%	Cyber/information security	33%	Digital business initiatives	32%	Enterprise resource planning	22%
6	Mobile applications	28%	Cloud services/solutions	31%	Customer/user experience	30%	Automation	20%
7	Artificial intelligence/machine learning	28%	Core system improvements/ transformation	27%	Artificial intelligence/ machine learning	27%	Infrastructure/data center	20%
8	Automation	25%	Automation	24%	Mobile applications	22%	Customer/user experience	19%
9	Cloud services/solutions	24%	Infrastructure/data center	23%	Automation	22%	Technology integration	19%
10	Infrastructure/data center	22%	Mobile applications	22%	Technology integration	21%	Software development/ upgrades	18%

Base: All answering, excluding prefer not to answer; n varies by segment.
Showing the 10 most common answers per segment. Multiple responses allowed; pick from a list.
Q: What are the technology areas where your organization will be spending the largest amount of new or additional funding in 2019?

Importance and Change in Risks During 2017

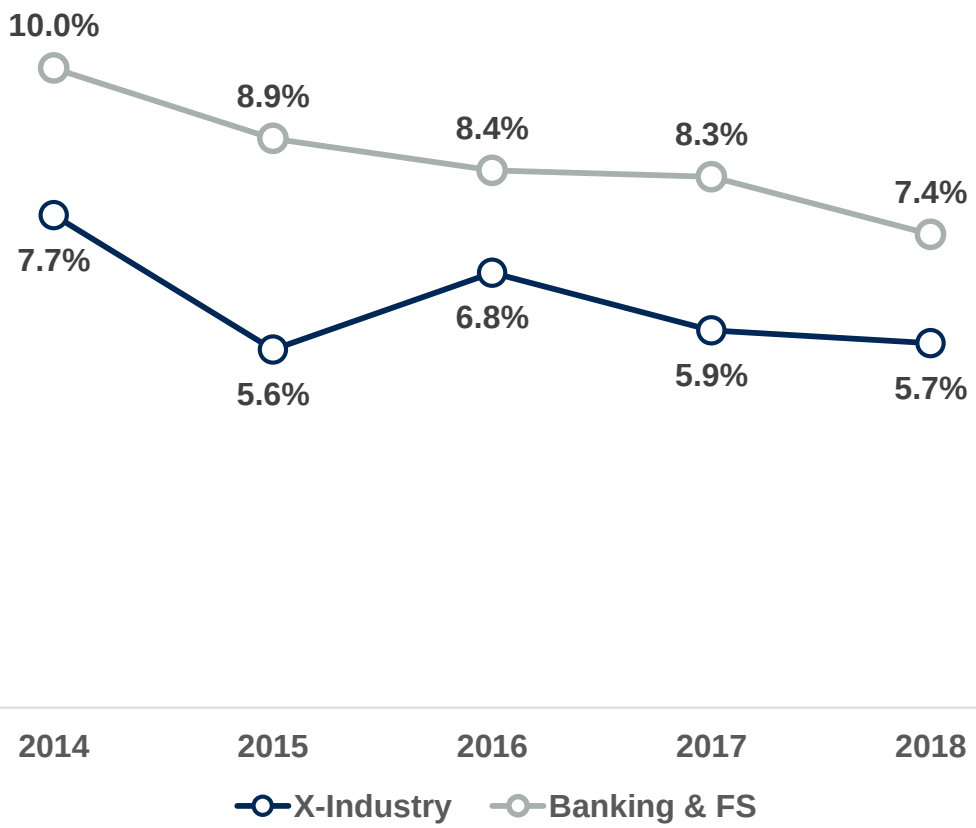


Expected Changes to Security Budgets

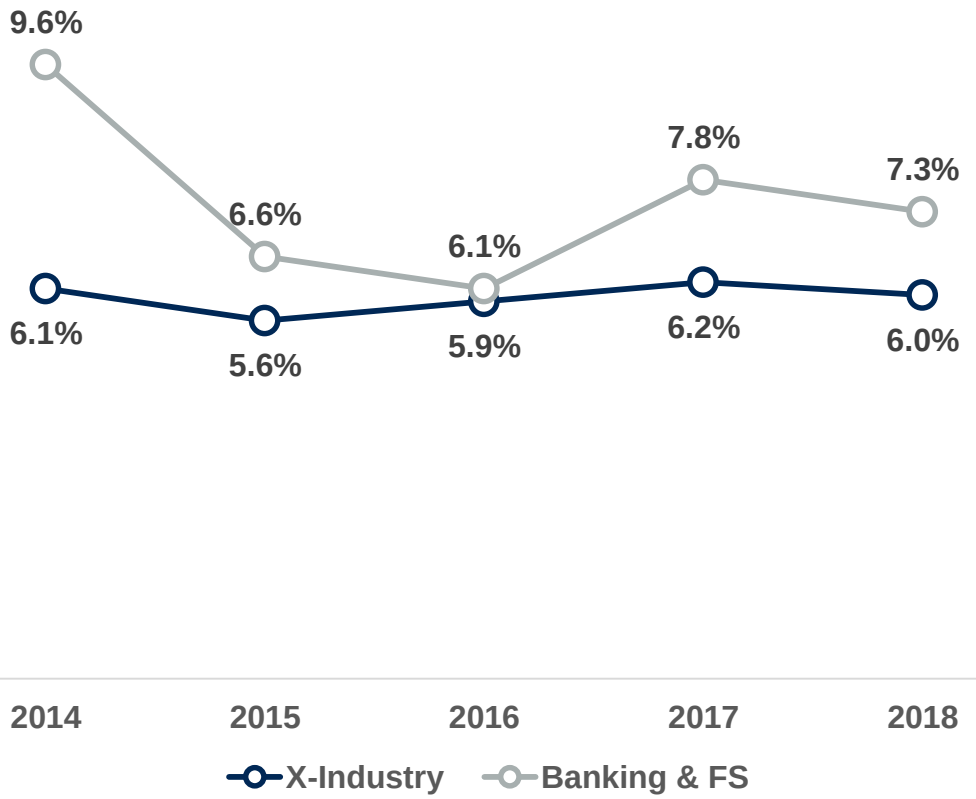


But Real Figures Show Otherwise…

IT Security Support FTEs as a Percent of Total IT FTEs



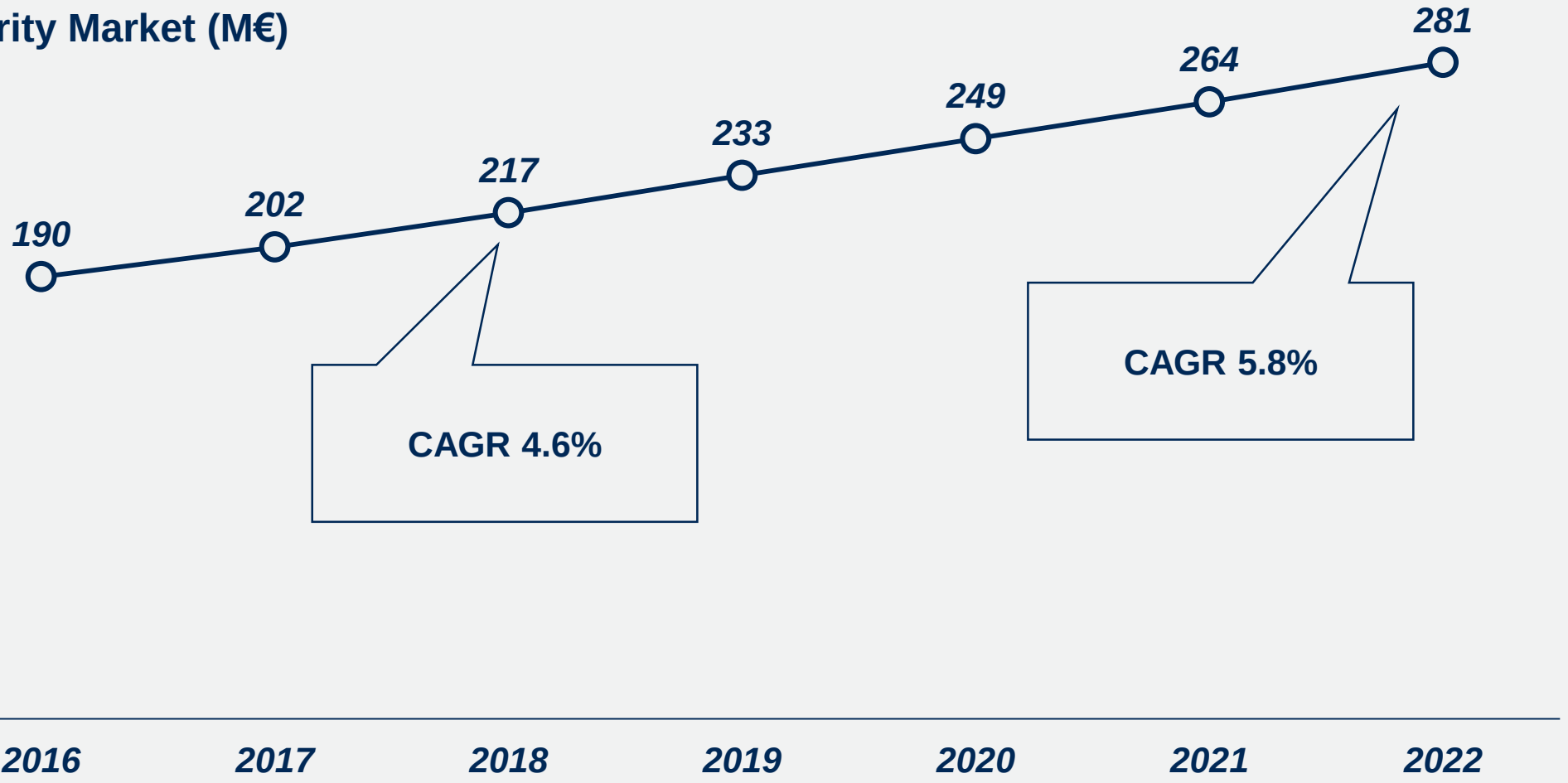
IT Security Spending as a Percent of IT Spending



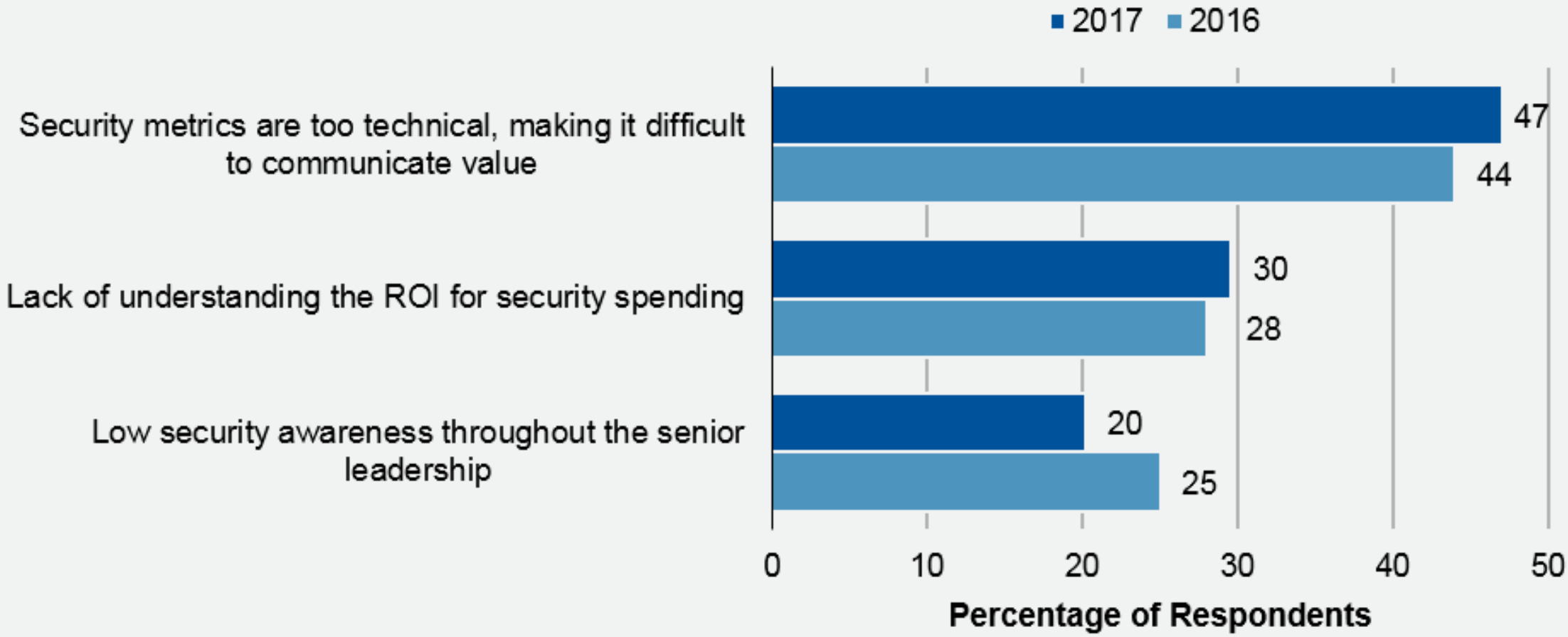
Gartner®

Security Market in Portugal

Overall Security Market (M€)

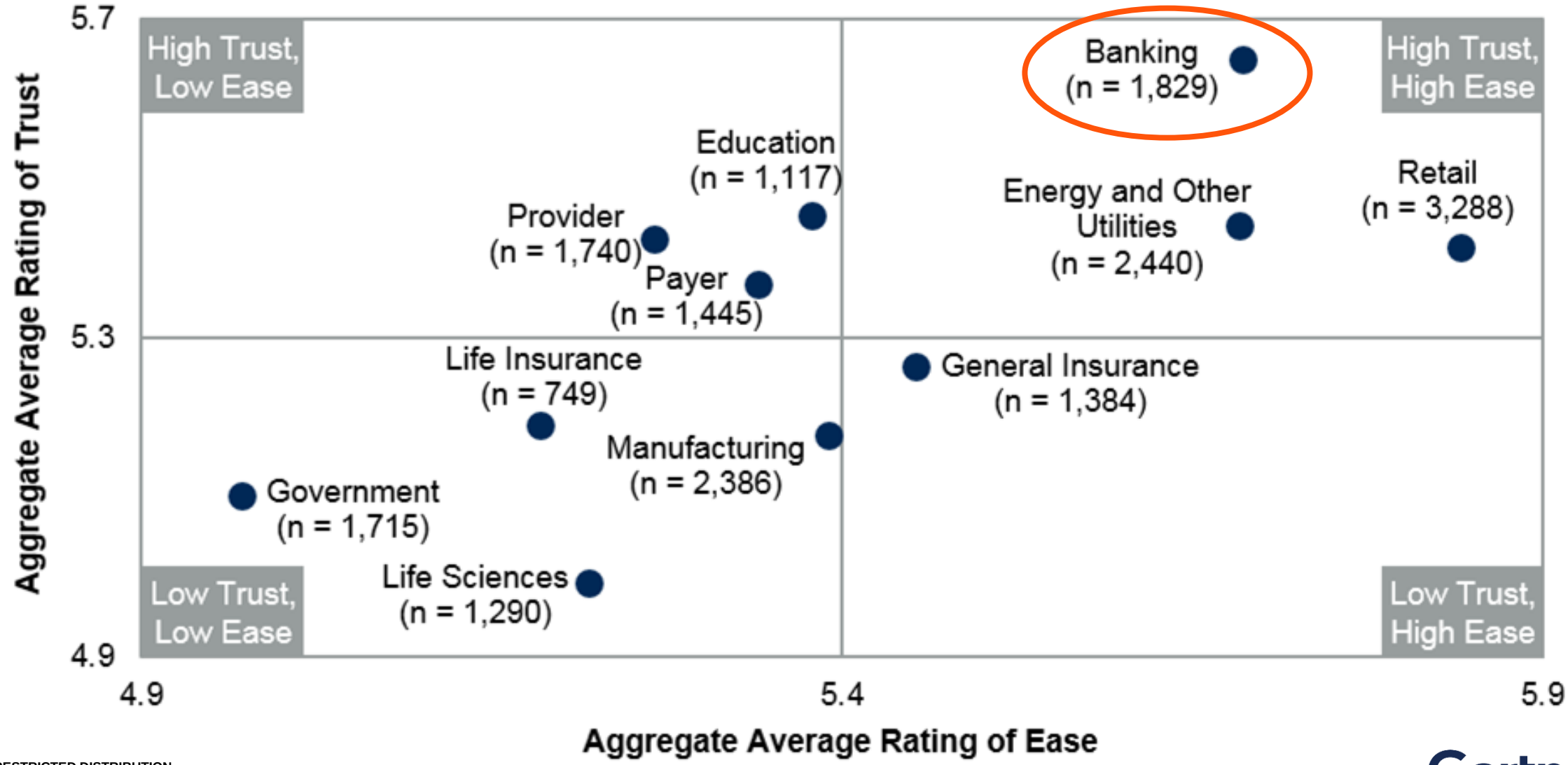


Top Challenges in Obtaining Security Budget



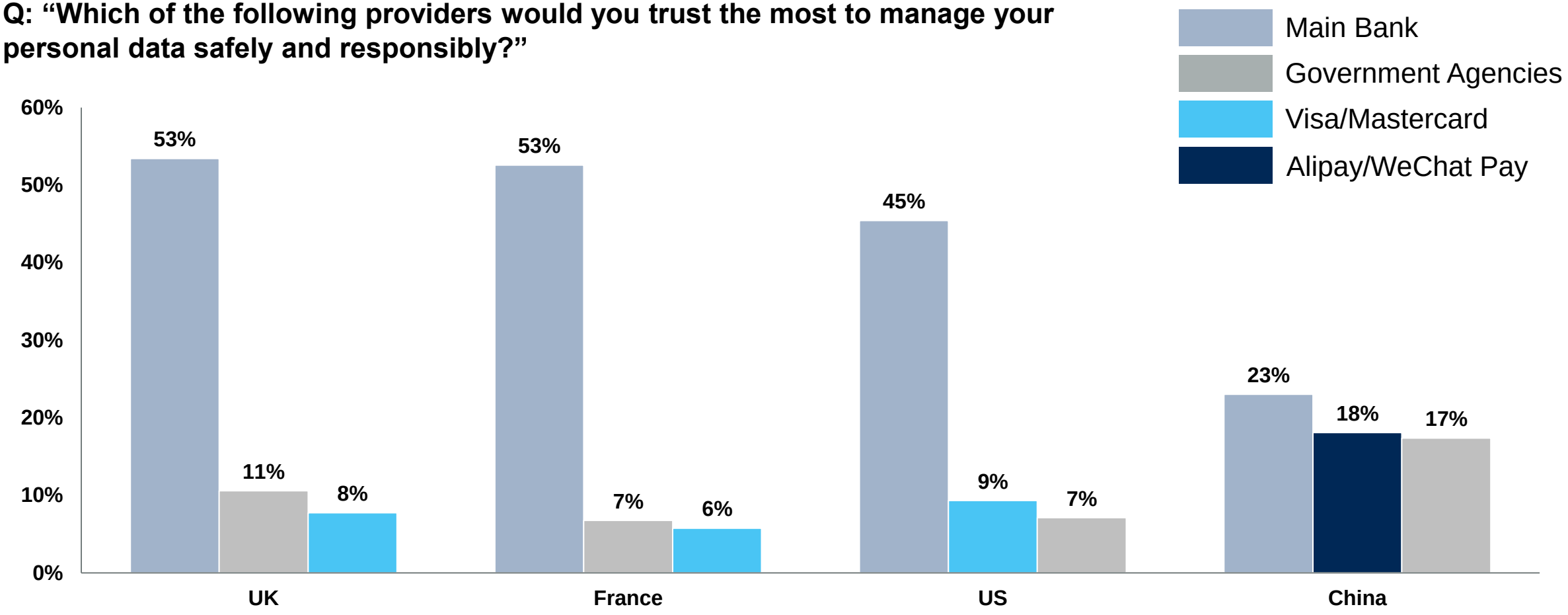
But this doesn't seem to impact customers' Trust in their banks…

Banks Are Well-Positioned on Trust and Ease



Building and Managing Your "Privacy Brand"

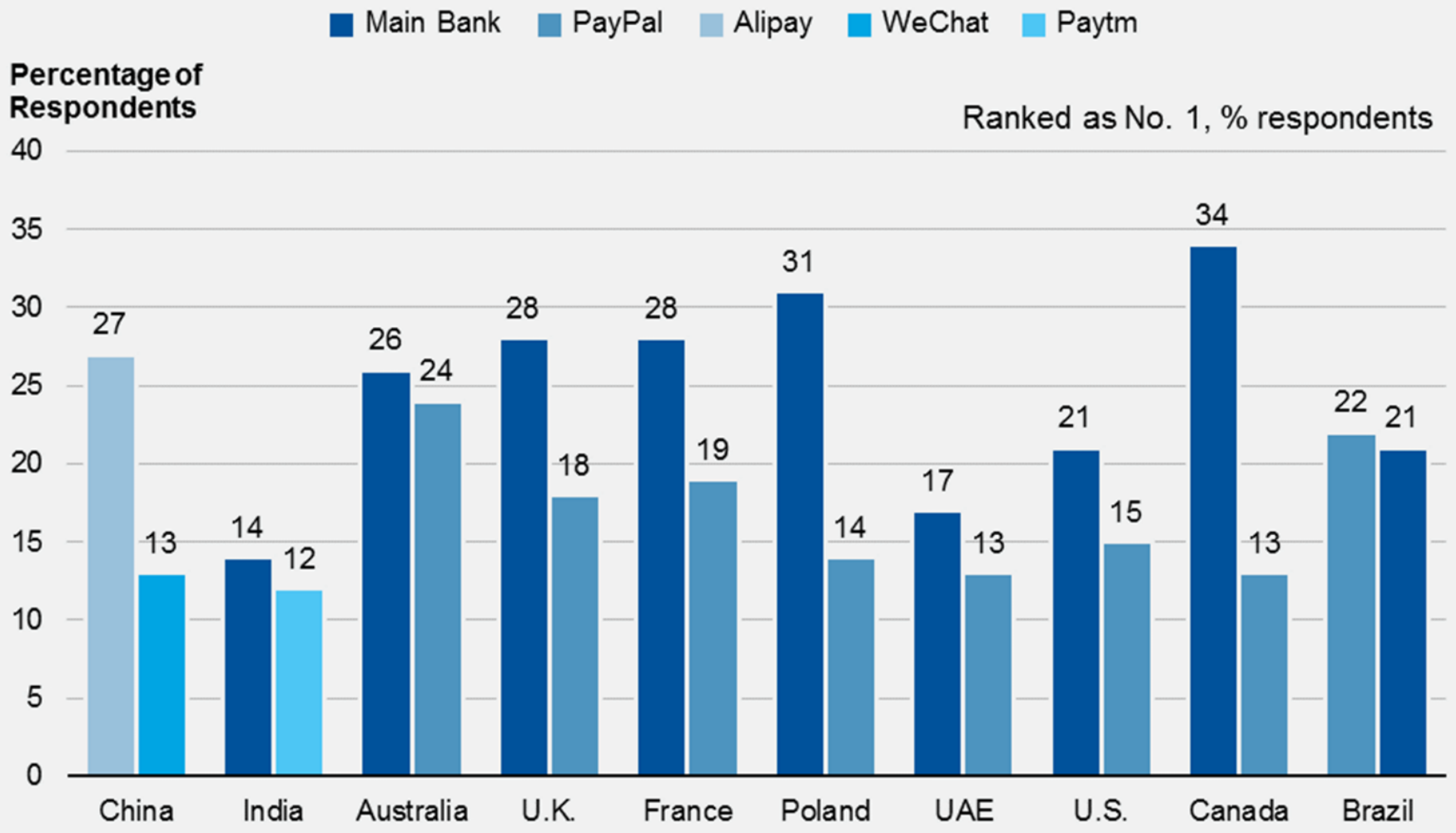
Q: "Which of the following providers would you trust the most to manage your personal data safely and responsibly?"



Source: Financial Services Digital Banking and Payment 4Q18

Gartner®

Trust in Banks - Payments

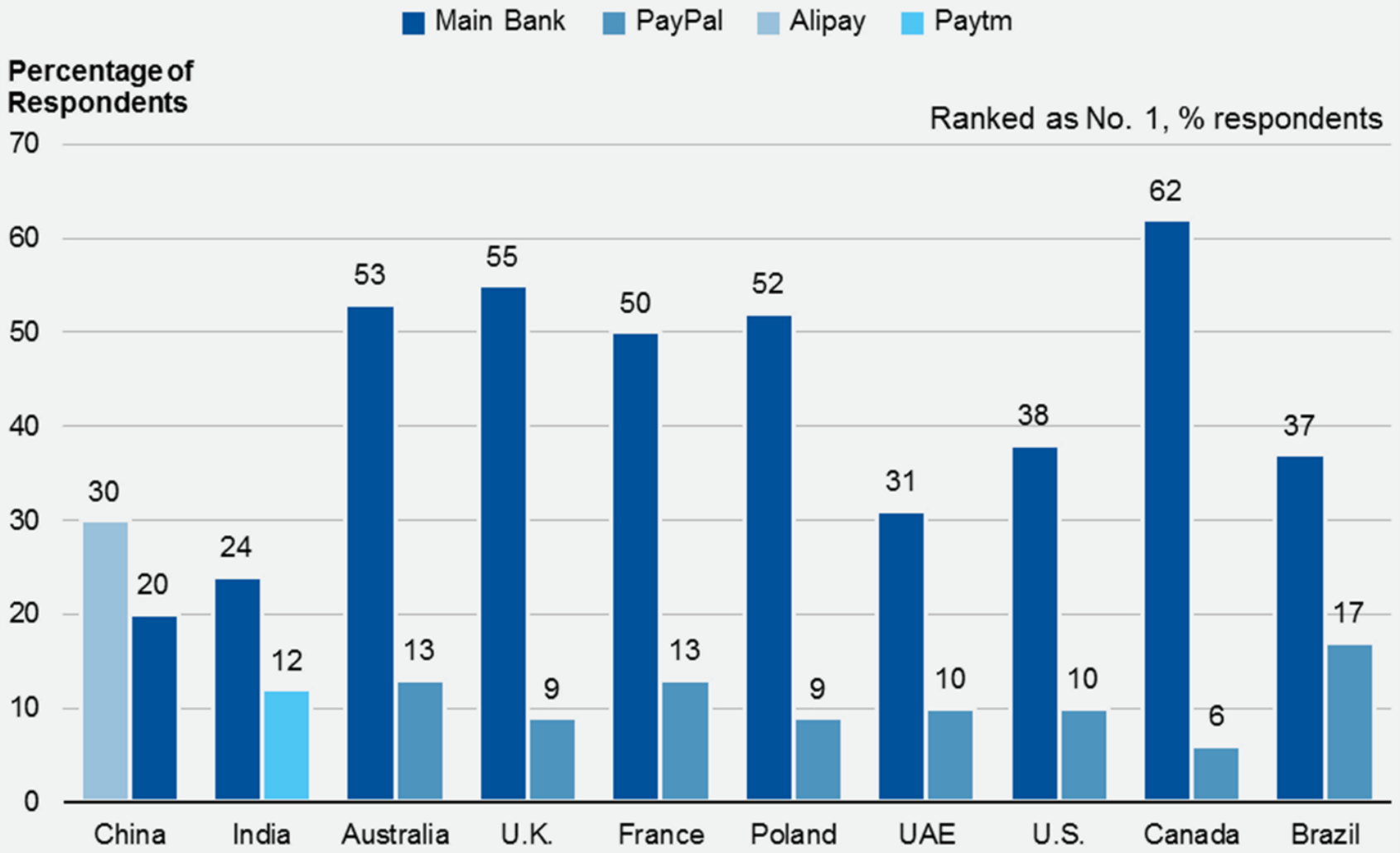


Question:

Which of the following would you trust the most to provide you with a better, more convenient payment solution?

From Gartner's 2017 Digital Banking and Payment SurveySample sizes: U.S. (n = 1,008), Canada (n = 1,007), U.K. (n = 1,006), France (n = 1,004), Poland (n = 1,005), UAE (n = 547), India (n = 1,010), China (n = 1,007), Australia (n = 1,006), Brazil (n = 1,046)

Trust in Banks – Current Accounts

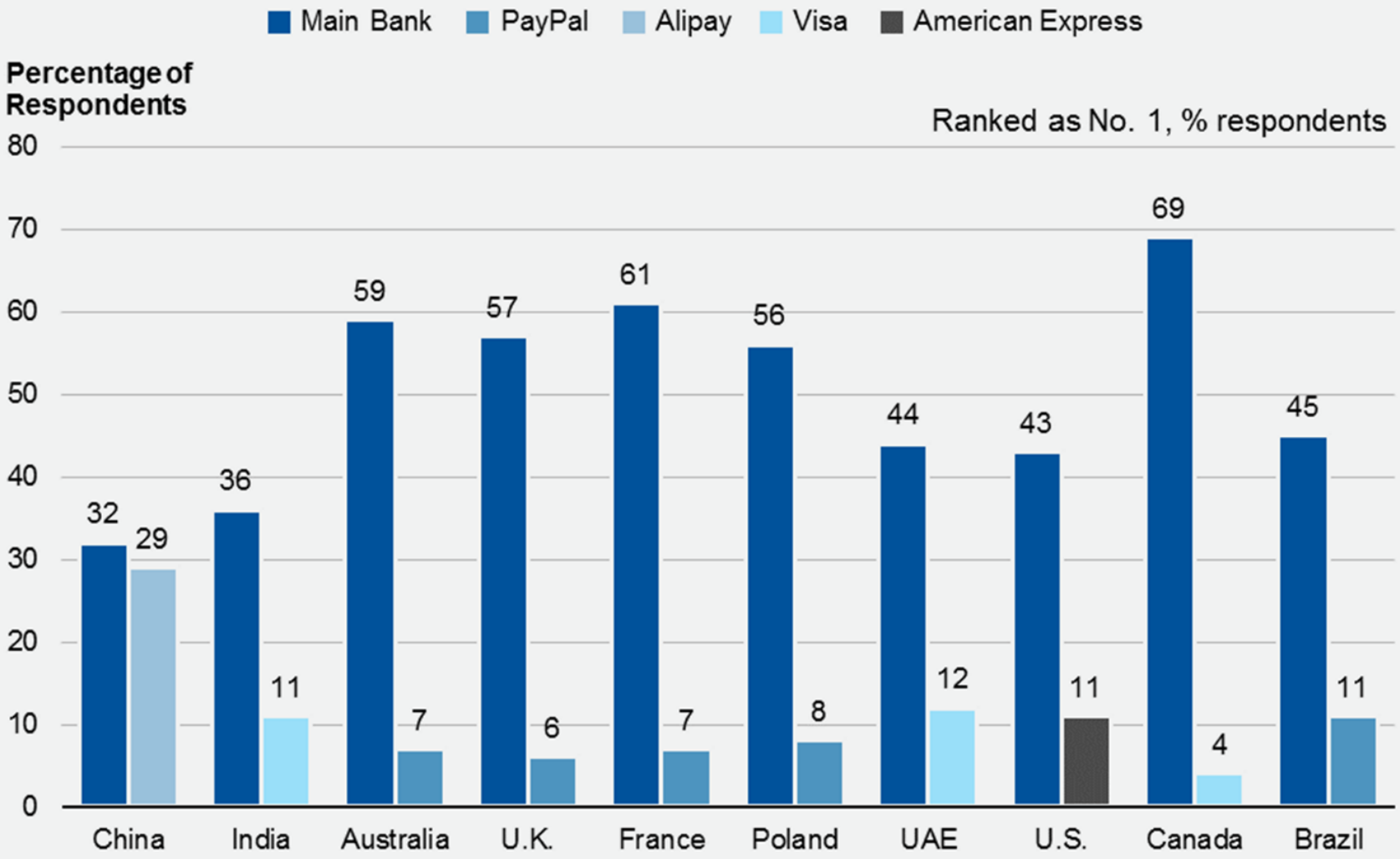


Question:

Which of the following would you trust the most to provide your Current Account/ Checking Account ?

From Gartner's 2017 Digital Banking and Payment SurveySample sizes: U.S. (n = 1,008), Canada (n = 1,007), U.K. (n = 1,006), France (n = 1,004), Poland (n = 1,005), UAE (n = 547), India (n = 1,010), China (n = 1,007), Australia (n = 1,006), Brazil (n = 1,046)

Trust in Banks – Financial Advisor



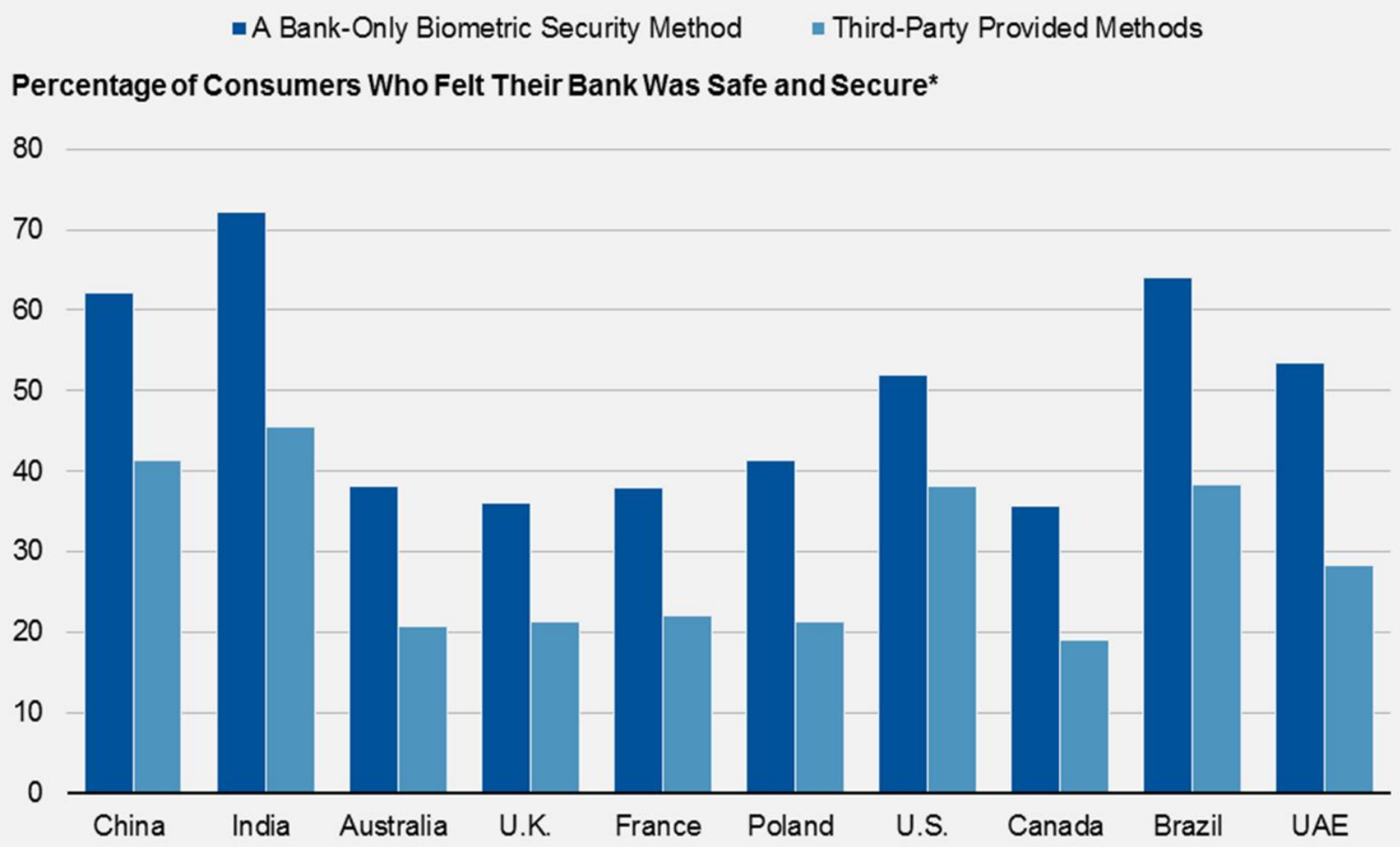
Question:

Which of the following would you trust the most to become your Main financial Service Advisor?

From Gartner's 2017 Digital Banking and Payment SurveySample sizes: U.S. (n = 1,008), Canada (n = 1,007), U.K. (n = 1,006), France (n = 1,004), Poland (n = 1,005), UAE (n = 547), India (n = 1,010), China (n = 1,007), Australia (n = 1,006), Brazil (n = 1,046)

Gartner

Trust in Banks – Biometric Authentication

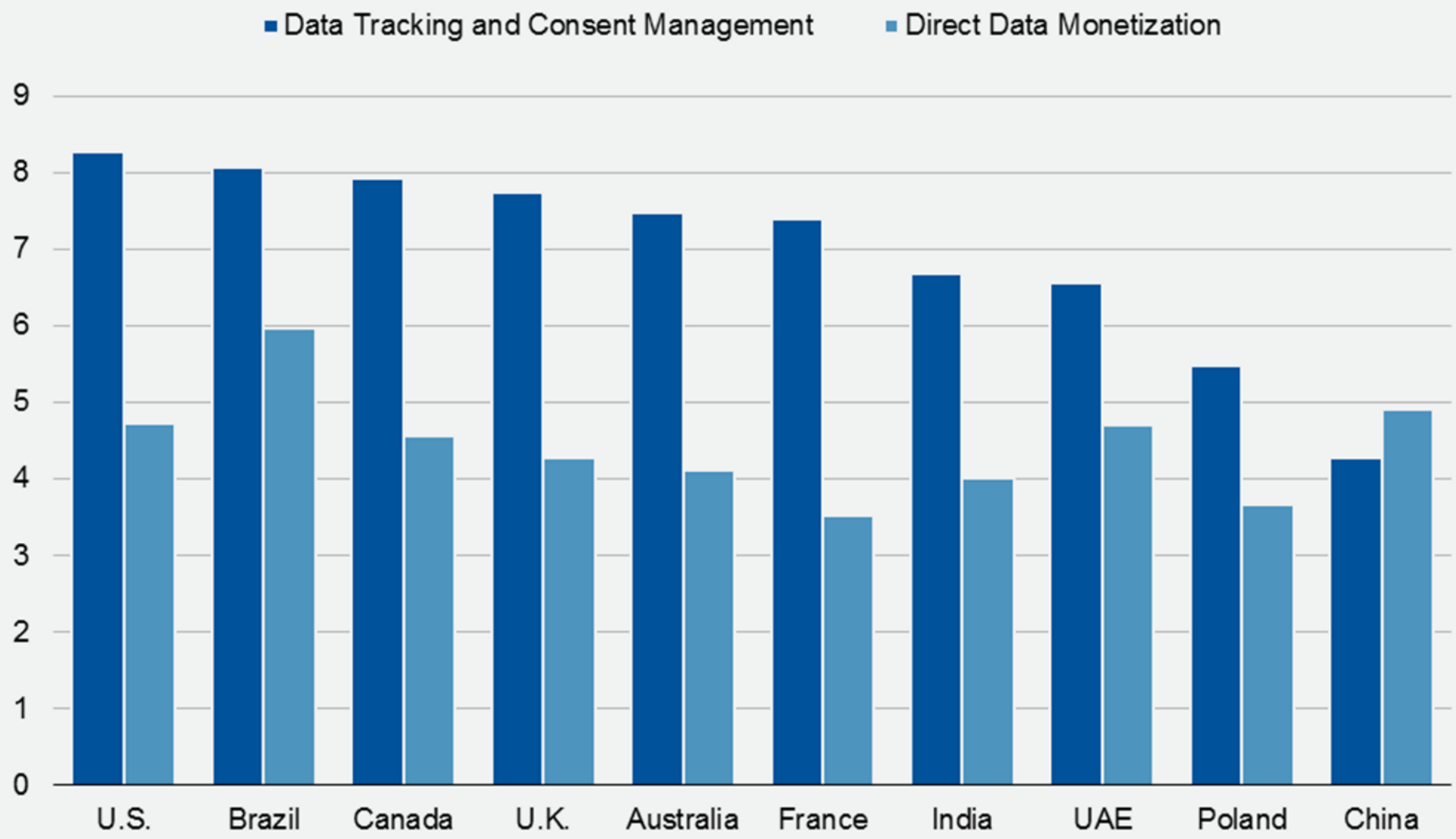


Question:

How Safe and Secure Do You Think Access to a Bank Would Be If the Bank Offered the Following Customer Authentication Solutions to You?

From Gartner's 2017 Digital Banking and Payment SurveySample sizes: U.S. (n = 1,008), Canada (n = 1,007), U.K. (n = 1,006), France (n = 1,004), Poland (n = 1,005), UAE (n = 547), India (n = 1,010), China (n = 1,007), Australia (n = 1,006), Brazil (n = 1,046)

Consent vs Data Monetization



Gartner®

By 2022, digital businesses with great customer experience during identity corroboration will earn 20% more revenue than comparable businesses with poor customer experience.

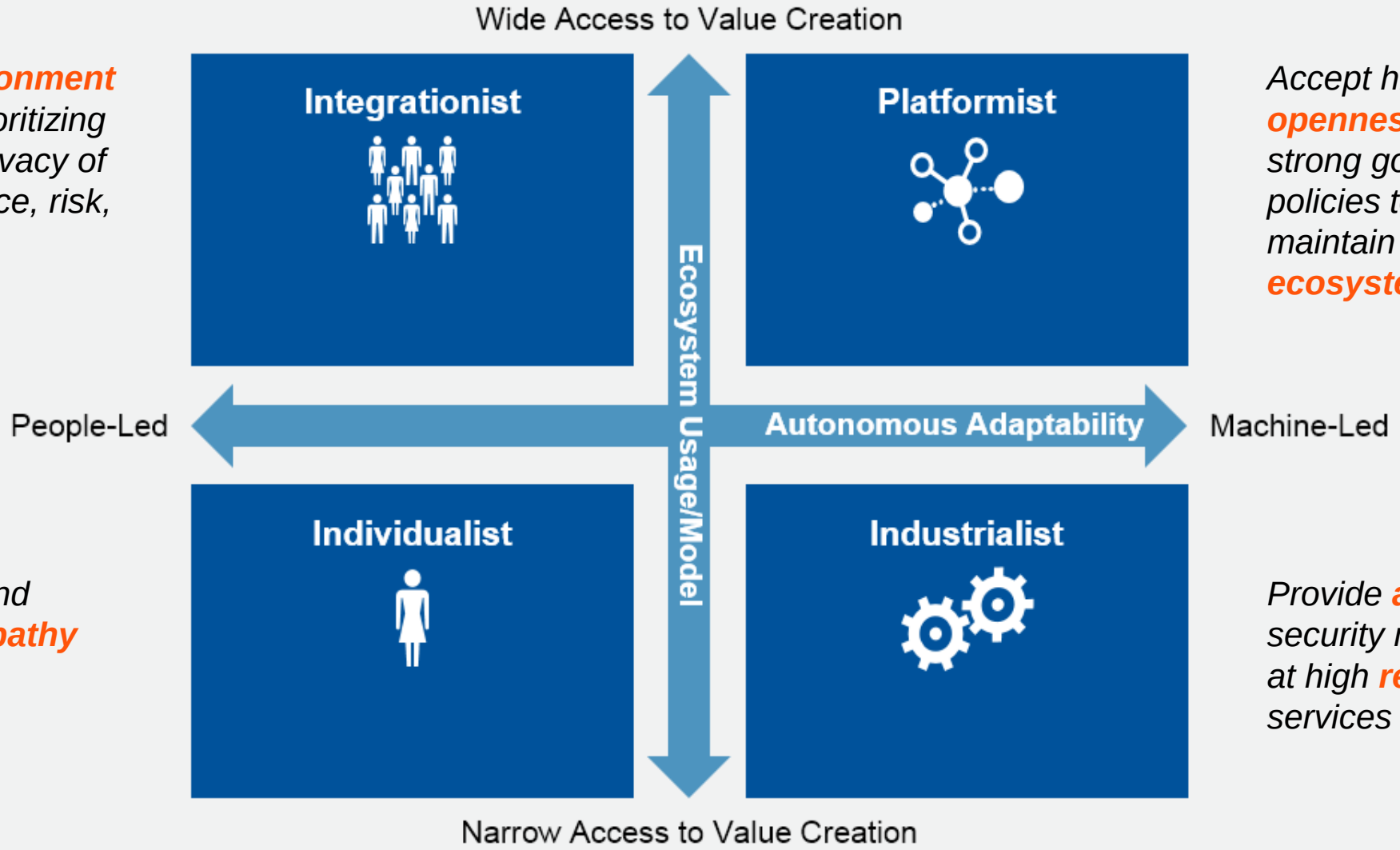
Trust and Resilience at the center of your cybersecurity strategy

CIA-PSR Model for Cybersecurity

Gartner®

What about ten years from now?

2030 Banking Scenarios



*Build an "**environment of trust**" by prioritizing security and privacy of data, governance, risk, and control*

*Accept high degrees of **openness** but establish strong governance policies to create and maintain **trust in the ecosystem***

*Align Privacy and Security to **empathy** and **relevance***

*Provide **affordable** security mostly aimed at high **reliability** of services*

What can be done now?

Let's be pragmatic and let's focus on a primary common objective…

Gartner®

Let's Keep Our Jobs!!!

Gartner®

By 2022, 50% of CEOs who lack cybersecurity postures that are defensible to their key stakeholders will be fired following material breach incidents that impact greater than 25% of their customer base.

Executive Fires over Security incidents 2012-2017

Eight Related Causes of Security Failure

Gartner®

Eight Related Causes of Security Failure

Example: Refusal to shut down a server for proper patching.

Example: Explicitly choosing to keep working on old hardware and software to save budget.

This situation leads to a false sense of security; lack of visibility results in such issues piling up without being addressed.

Make sure that invisible systemic risk is recognized, reported and discussed in governance processes related to addressing technology risk

Gartner

Eight Related Causes of Security Failure

Example: "what idiot would build an unsecure application?"

Example: "Well, why don't you fix it? Why are you telling me? Isn't it your job?"

This often results in security being thought of as "somebody else's problem."

Put technology risk and cybersecurity into a business context so decision makers can better understand how their decisions impact their desired business outcomes.

Gartner

Eight Related Causes of Security Failure

Example: "there — surely that's enough to keep us out of the headlines and protect the organization!"

Executives who are willing to raise operational costs while negatively impacting business operations are not positioned to make defensible decisions where security is concerned.

Organizations should avoid heavy investments that themselves damage the ability to achieve desired business outcomes.

Gartner

Eight Related Causes of Security Failure

Example: A security officer blocks the release of a critical application due to security concerns that show little or no consideration of the business outcomes the application supports.

CISO acting as defenders will not negotiate appropriate business controls, which leads to poor security investments. It also puts security people in charge of protecting business outcomes they do not understand, which in turn leads to more invisible systemic risk.

Make sure that security does not act as a defender but rather as a facilitator of decisions that balance the need to protect against the need to run the business.

Gartner

Eight Related Causes of Security Failure

Example: “You’re not going to do that on my watch. That will ruin my customer experience!”

Executives only owning the profit and loss responsibility for the application and had no responsibility, accountability or interest in the application’s level of security.

If accountability means that someone will get fired if something goes wrong, then no one will engage and everyone will continue to be trapped in a cycle that is no longer defensible for CEOs, boards and senior executives.

Gartner

Eight Related Causes of Security Failure

Example: “Where is that form I need to sign that makes this go away?”

A risk-appetite statement works well when it has a measurable scale of risk and governance process that supports defensible decision making.

Create mechanisms that allow for the acceptance of risk within defined parameters.

Gartner

Eight Related Causes of Security Failure

Example: Society actually feels sorry for people who get robbed but not so much for cybersecurity incidents.

While this isn't fair, it's the result of decades of treating security as a black box. No one understands how it really works and, as a result, when an incident does occur the assumption is that someone must have made a mistake.

Society is not going to change until organizations and IT departments start treating and talking about security differently. Security is not a black box.

Gartner®

Eight Related Causes of Security Failure

Example: An executive blocks the simple message that "**there is no such thing as perfect security**" from a board presentation on the state of security.

It starts with transparency. Gartner has witnessed countless interactions with organizations that have boards and executives who do not want to hear or acknowledge that security is not perfect.

A willingness to understand and talk about the realities and limitations of how security works is necessary to tackle the challenges presented here.

Gartner

Wrapping Up

- ✓ Awareness is finally high, real commitment still low
- ✓ Banks are still largely trusted by clients, should leverage this and put trust at the hearth of their cybersecurity strategies
- ✓ CxOs need to start acting differently in order to deal with incidents… and keep their jobs!

Gartner®