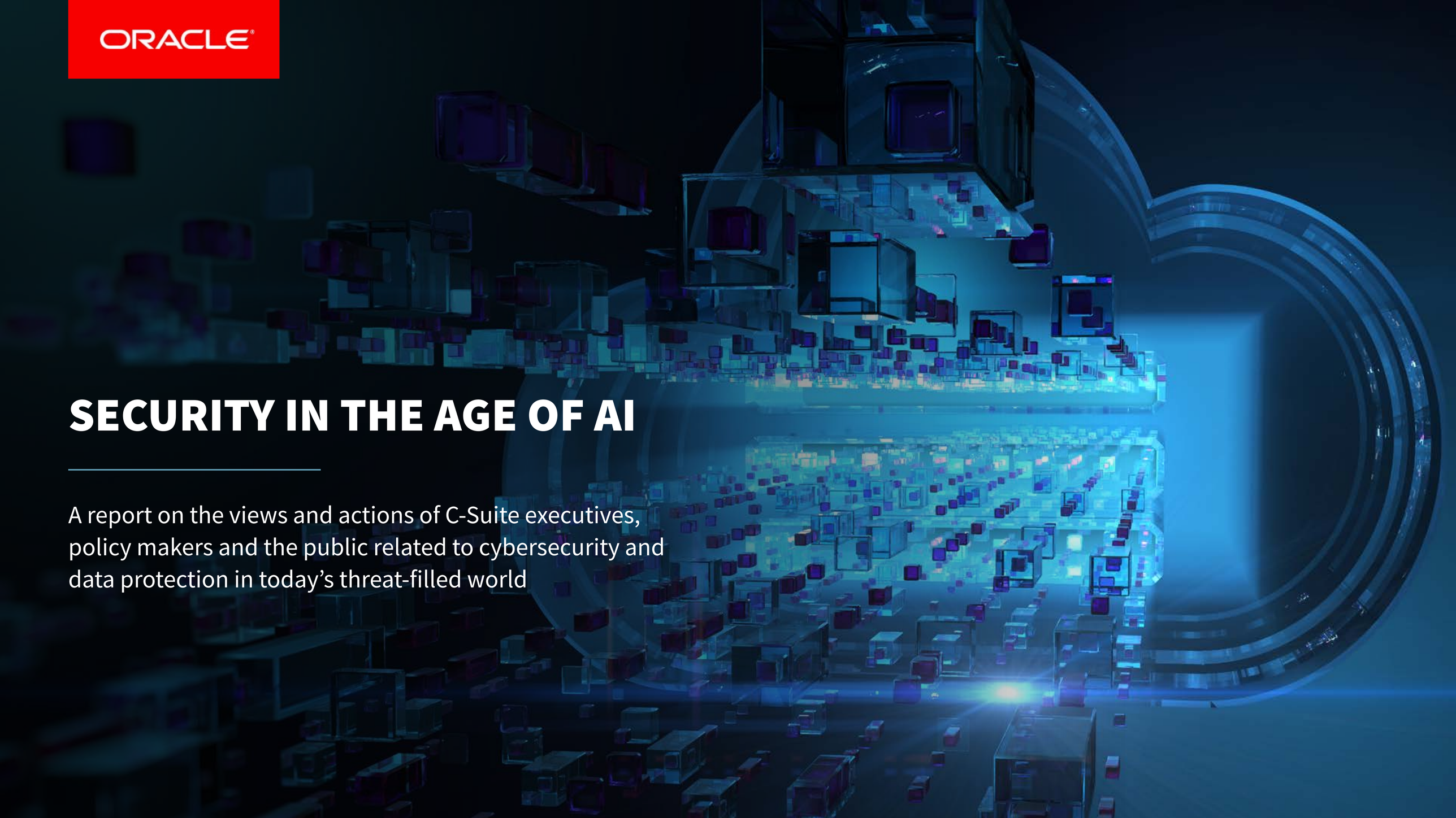


SECURITY IN THE AGE OF AI

A report on the views and actions of C-Suite executives, policy makers and the public related to cybersecurity and data protection in today's threat-filled world

Preface

I am proud to present Oracle's inaugural report on "Security in the Age of AI," which explores perceptions and actions being taken by C-Suite executives, policy makers and the general public to improve the state of America's cybersecurity.

As confirmed by this survey, security is a top priority for individuals and organizations across America. Citizens, enterprises and governments are operating in an increasingly complex cybersecurity landscape, facing growing threats from the full spectrum of malicious actors – from nation states to cybercriminals to hacktivists and insiders. It is estimated that cybercrime will cost the global economy $6 trillion annually by 2021.[1]

The current cyber environment is defined by unprecedented connectivity across billions of devices and sensors we rely on every day. Internet connected devices are expected to reach nearly 30 billion within the next three years[2], driven predominantly by growth in the Internet of Things (IoT) and supporting infrastructure advancements, such as 5G wireless systems. With more data to store, manage, and secure, enterprises face additional vulnerabilities for attackers to identify and exploit.

The cyber threat landscape has been tilted in favor of the bad actor, but the rules of the game are now changing. While cyber defense resources have grown at a much slower rate than the amount of data, number of devices, and breadth of users we protect, second-generation cloud architectures, powered by built-in artificial intelligence (AI) and machine learning (ML) capabilities, are driving a new era of data security. These next-generation cloud-based technologies not only enhance security capabilities significantly by addressing problems of scale, human error, and response time, they also free the workforce for more strategic, value-added tasks.

With this survey, we shed light on the attitudes and practices adopted by C-Suite executives, policy makers, and the general public in relation to data security, the challenges and opportunities they face, and the extent to which they are leveraging emerging cloud-based technologies to take cyber resilience to the next level.

More specifically, this survey informs us on:

- Views on top security vulnerabilities
- Who should be responsible for protecting our data
- Adoption of technology now available to combat today's threats

Our security challenges continue to mount. However, thanks to continued innovation in enterprise cloud architecture, we have an opportunity to prevail against today's threats. We believe the insights presented in this report will get us one step closer to understanding the threat landscape in which we operate, where security vulnerabilities lie, and the actions we as businesses, government and citizens need to take to effectively protect our critical enterprise systems.

Sincerely,
Edward Screven
Chief Corporate Architect, Oracle

[1] The 2019 Official Annual Cybercrime Report
[2] Ericsson Internet of Things Forecast

Who We Surveyed

341

C-Suite executives

110

Policy makers

324

General public

C-Suite executives

The CxO audience consisted of **341 CEOs and CIOs, at firms between 500 to 10,000 employees**, making between 100M to 999M dollars in revenue annually in a variety of industries, and located across the United States. They typically are early adopters of new technology and their firms store financial, customer, and operations data either on premise or in the cloud.

Policy maker audience

The policy maker audience consisted of **110 well-educated government employees that worked in IT, legal or administration**, typically providing services to the federal or state government and resided in New York, Virginia, or Maryland. They typically store consumer data and are much more risk averse when it comes to adopting new technologies, usually being the last sector surveyed in this study to adopt new technologies.

General public

The general public audience consisted of **324 educated, technologically or politically savvy individuals working in non-managerial roles** at firms in various industries across the United States.

Executive Summary

The majority of C-Suite executives and policy makers in the United States believe investing in security software, infrastructure and emerging technologies is paramount to protecting U.S. data from growing cybersecurity risks.

- When asked what would make the U.S. government better equipped to secure data, a majority of C-Suite executives and policy makers agree that investing in IT/security infrastructure (51 and 62 percent respectively) and security software (59 and 60 percent respectively) is critical.
- When it comes to their own security investments over the next 24 months, 44 percent of C-Suite executives and 33 percent of policy makers plan to purchase new software with enhanced security; and 37 percent and 25 percent, respectively, plan to invest in new infrastructure solutions to improve security.
- When asked what their organization has done over the past five years to improve security, policy makers cite upgrading existing software (52 percent) and training existing staff (50 percent), but only 41 percent have purchased new software with enhanced security features and only 27 percent have invested in new infrastructure solutions.

Both C-Suite executives and policy makers rank "human error" as the top cybersecurity risk for their organization. As a result, they prioritize investing in people (via training and hiring) to improve security, more than security-advancing technology, such as new software, infrastructure, and artificial intelligence (AI) and machine learning (ML), even though these technologies have the ability to significantly minimize or eliminate human error entirely.

- When asked what they plan to do in the next 24 months to improve their organization's security, "training existing staff" was the top choice for both C-Suite executives and policy makers. Purchasing AI/ML or new infrastructure solutions were less prioritized.
- 80 percent of policy makers and nearly 70 percent of C-Suite executives have not adopted and/or implemented AI/ML to its fullest potential.
- When asked, they agree that these same cloud-based technologies are critical to improving their cybersecurity defenses, with six in ten C-Suite executives and policy makers citing security as the top benefit of cloud technology.

The technology industry is one of the most trusted sectors of business for responsibly protecting America's data.

- 78 percent of C-Suite executives, 75 percent of policy makers and 63 percent of the general public believe the technology industry is well equipped to protect data.
- 79 percent of C-Suite executives and policy makers, and 64 percent of the general public trust the technology industry to behave responsibly and in the best interests of the American public, as it relates to data security.
- Federal government is among the least trusted by all survey respondents, including the policy makers themselves.

Respondents believe foreign governments pose the biggest threat to the technology industry.

- Nearly 40 percent of policy makers cite "attacks and hacking by foreign governments" as the top security challenge facing the technology industry.

Most survey respondents believe businesses should bear the responsibility of data protection.

- Only about one in three C-Suite executives or policy makers think it is the government's responsibility to protect consumer data.

A majority of the respondents believe autonomous technologies will benefit the U.S. economy, with "increased productivity" cited as the top benefit. Yet, the general public has mixed feelings about the technology's impact on their professional lives

- C-Suite executives expect IT services, data management, and manufacturing functions to be fully autonomous in the next five years.
- Nearly 80 percent of the general public think autonomous technologies will have a positive impact on the U.S. economy.
- Additionally, around 40 percent of the general public feel that autonomous technologies will leave them behind, as opposed to creating opportunities for them.

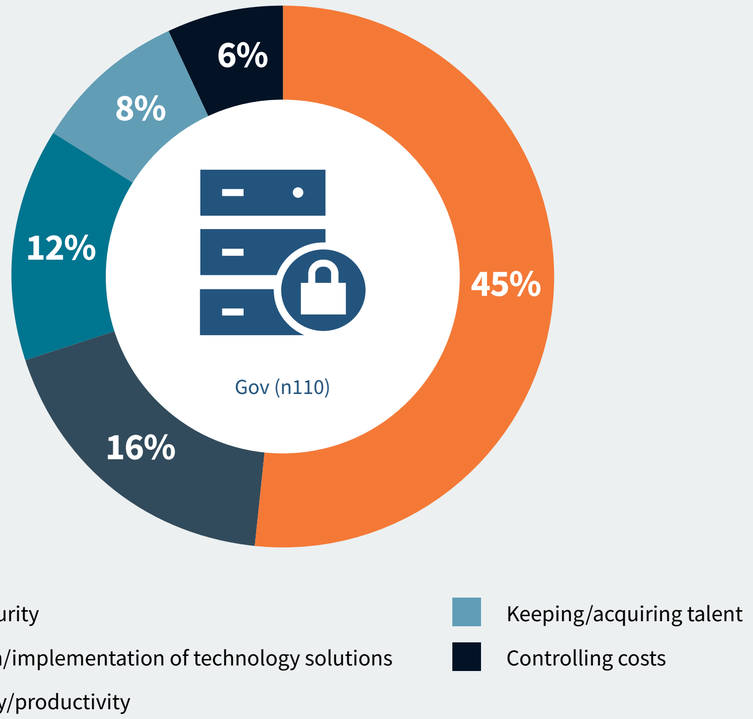
While a majority of C-Suite executives and policy makers have not adopted or implemented AI/ML to their fullest potential, they strongly believe autonomous technologies powered by AI/ML will improve the way they protect and defend against security threats.

- When asked about the most significant future benefit of autonomous technologies to companies or organizations, "improving security" was a top choice for both C-Suite executives and policy makers, along with "improving efficiency/productivity."
- An overwhelming majority of C-Suite executives (82 percent) agree that autonomous technologies will improve security and increase trust in the way companies handle sensitive information.
- "Increased level of security" is seen as the primary benefit of autonomous security by nearly half of the C-Suite executives and policy makers.

Securing Data Is Now Policy Makers' Top Priority

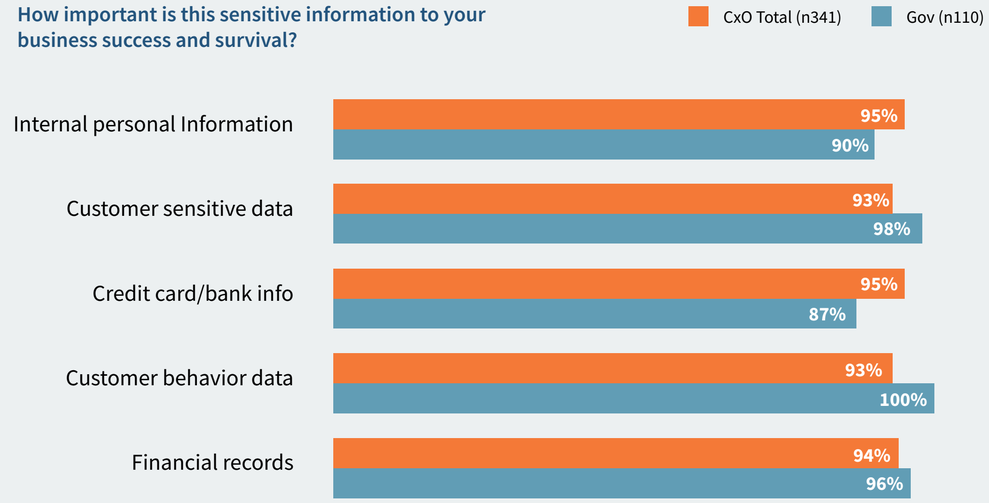
Given the frequent and massive data breaches, increasingly sophisticated hackers and growing privacy leaks, it is no surprise that policy makers cite data security as their top organizational priority, more critical than attracting talent and controlling costs.

Thinking back on everything that you have read, heard, and seen over the last 12 months, which of the following is the biggest concern for your organization over the next 12-24 months?

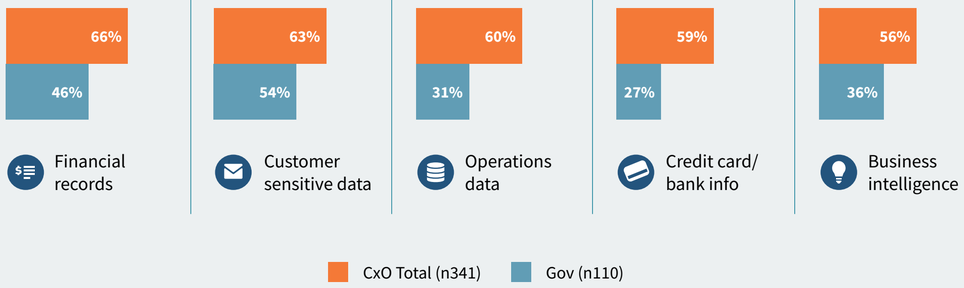


The data that companies and policy makers have within their walls are critical to their success…

How important is this sensitive information to your business success and survival?

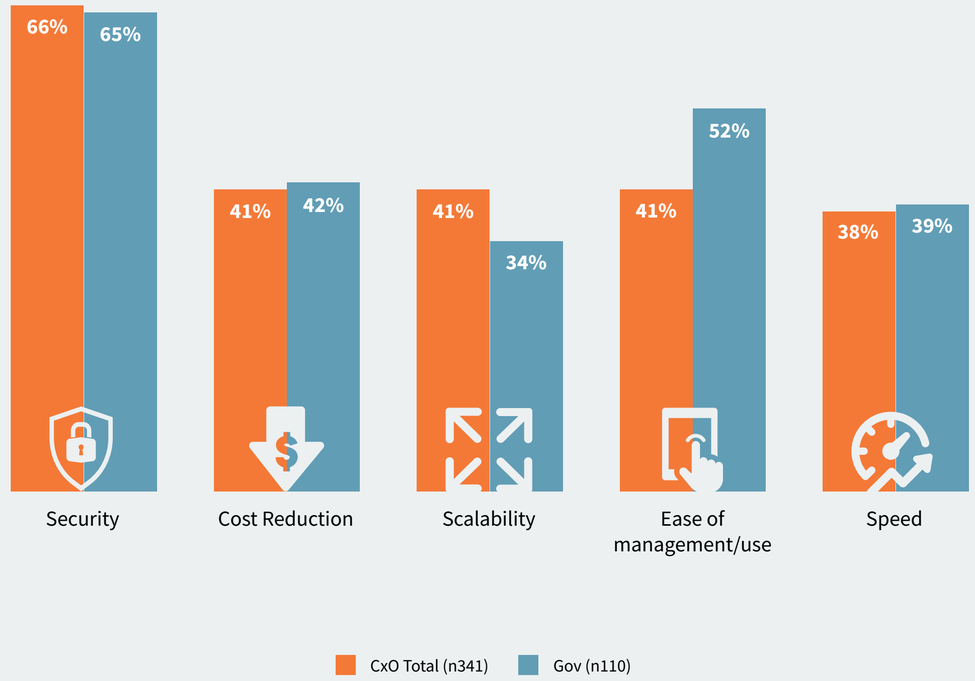


Which of the following types of sensitive information do you use and store at your business?



…and more than **six in ten C-Suite executives and policy maker respondents** cite security as the top benefit of cloud technology.

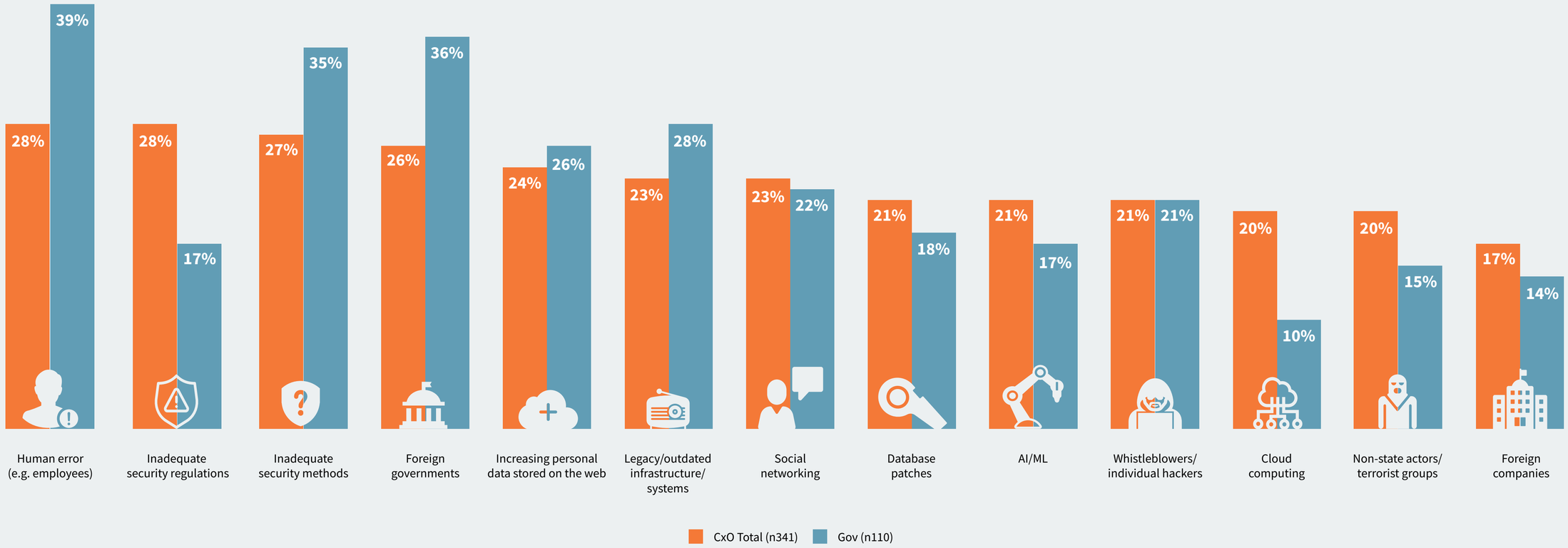
What are the biggest benefits of cloud computing for your organization today?



‘People’ Seen as Biggest Security Vulnerability, Yet C-Suite and Policy Makers Invest Disproportionately in People Over Technology to Solve Security Issues

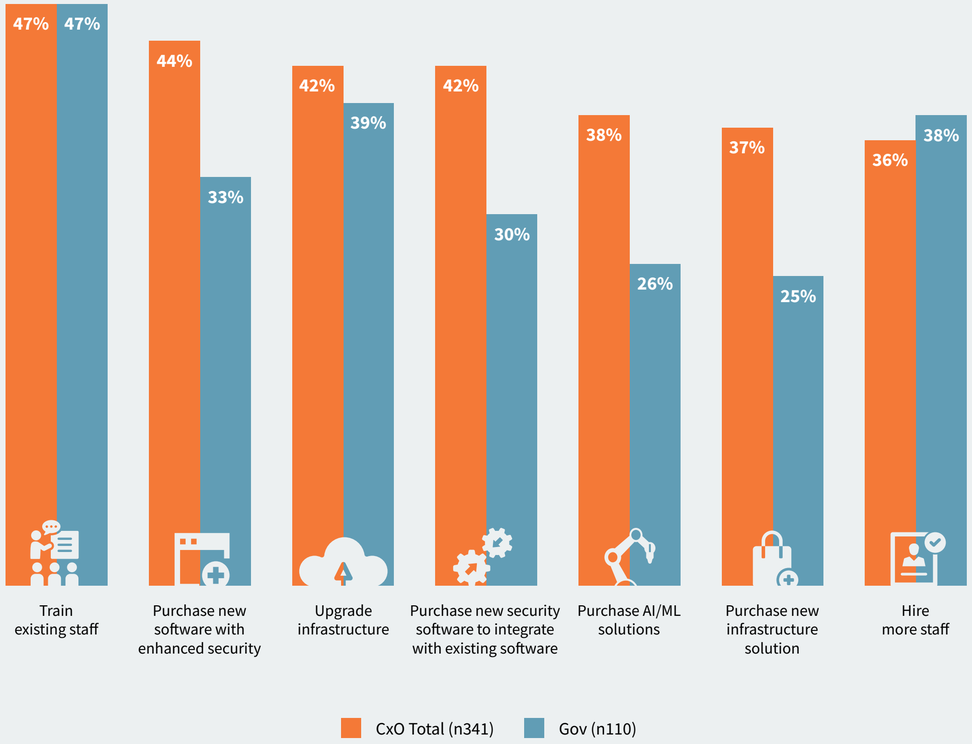
When asked about security vulnerabilities, employees are seen as the biggest risk in our cybersecurity defenses across America, according to both C-Suite executives and policy makers…

Which of the following vulnerabilities causes the greatest potential information security risk for your organization?

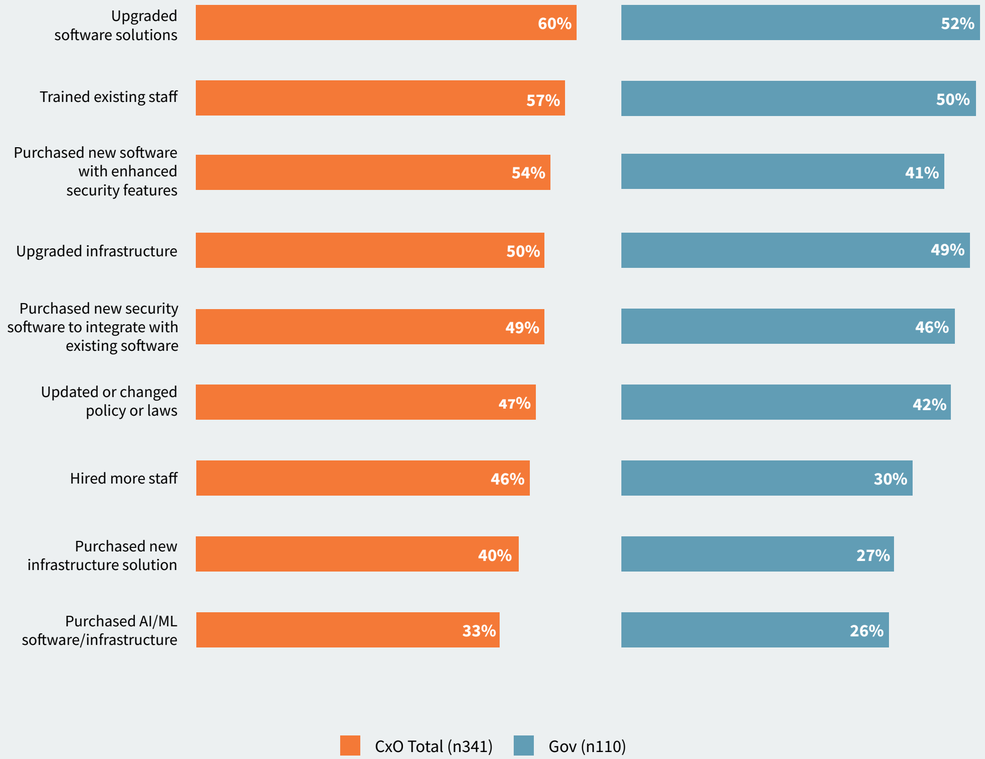


Both C-Suite executives and policy makers rank “human error” as the top cybersecurity risk for their organizations. However, in the next two years, they are choosing to invest more in people—via training and hiring—than in technology, such as new types of software, infrastructure, and AI/ML, which is essential to advancing security and significantly minimizing human error.

Which of the following is your organization planning on doing in the next 24 months to improve security?

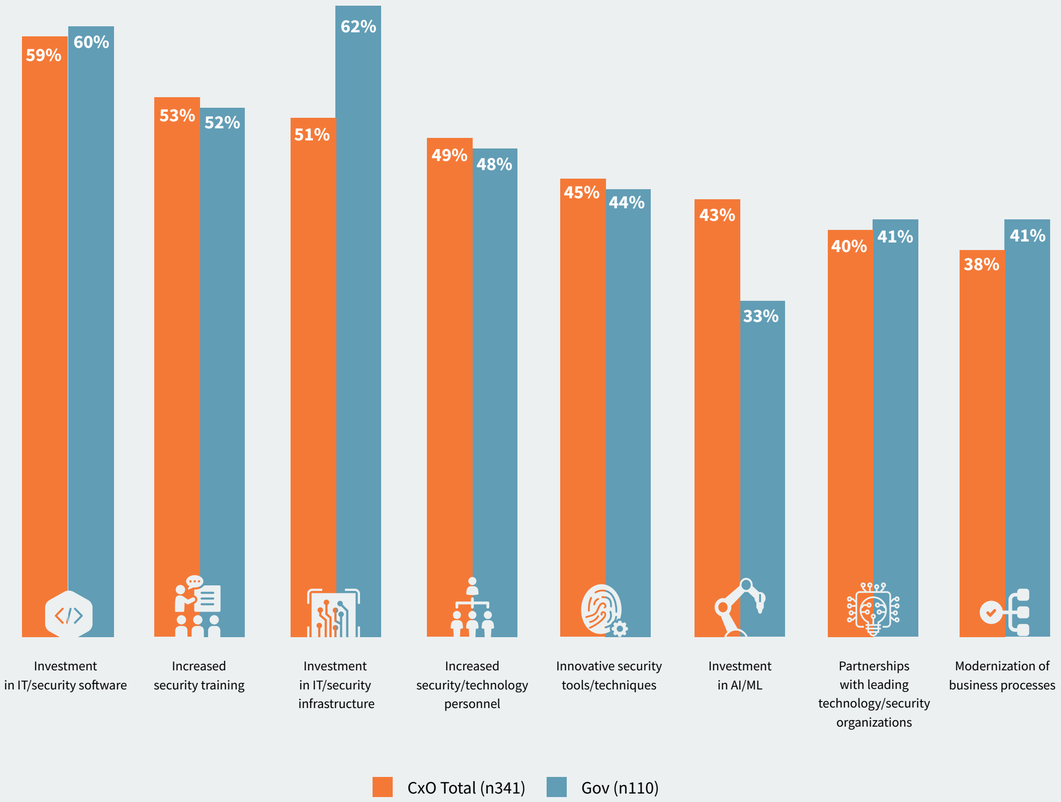


Which of the following has your organization done in the past 5 years to improve security?



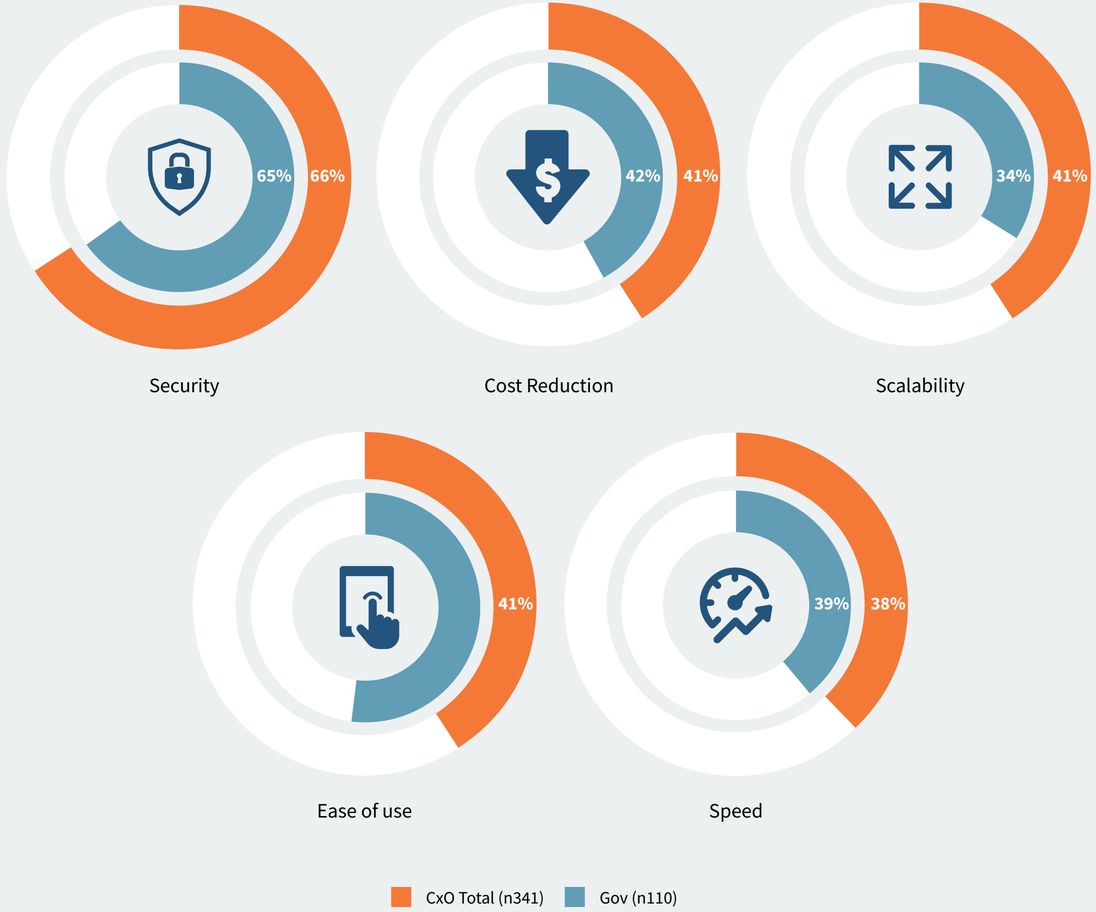
Yet, when asked what the U.S. government needed to keep the country's data safe from attackers, **six in ten respondents** say that investing in emerging cloud-based technologies is paramount...

Which of the following would make the U.S. government more equipped at securing data?



C-Suite executives and policy makers also cite security as the top benefit of cloud technology.

What are the biggest benefits of cloud computing for your organization today?

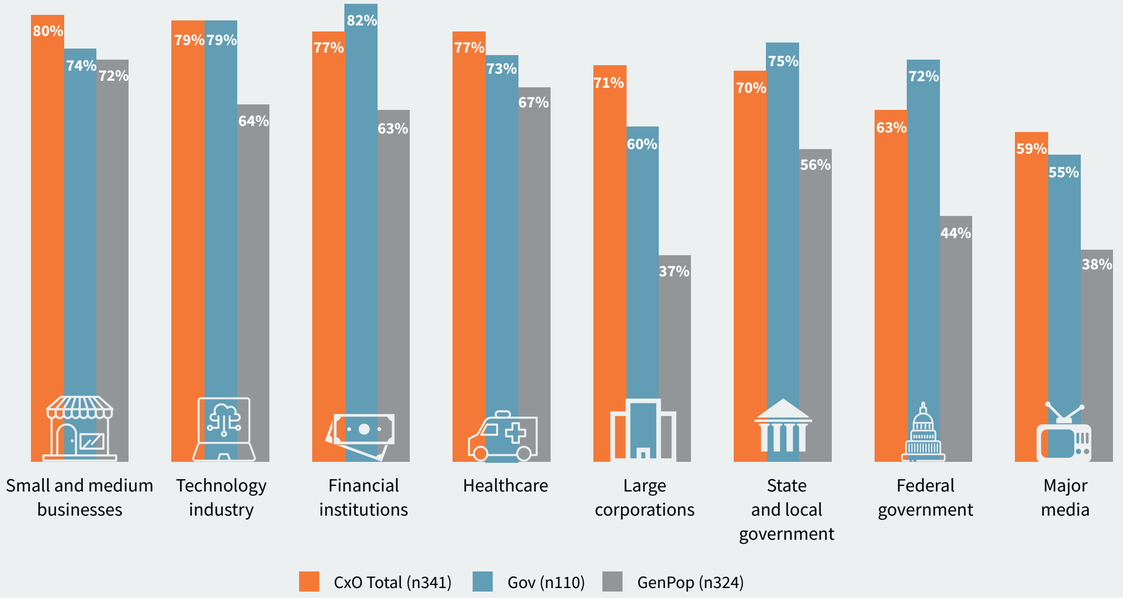


Trust in Organizations' Ability to Protect Data

The technology industry is one of the most trusted sectors of business for responsibly protecting America's data.

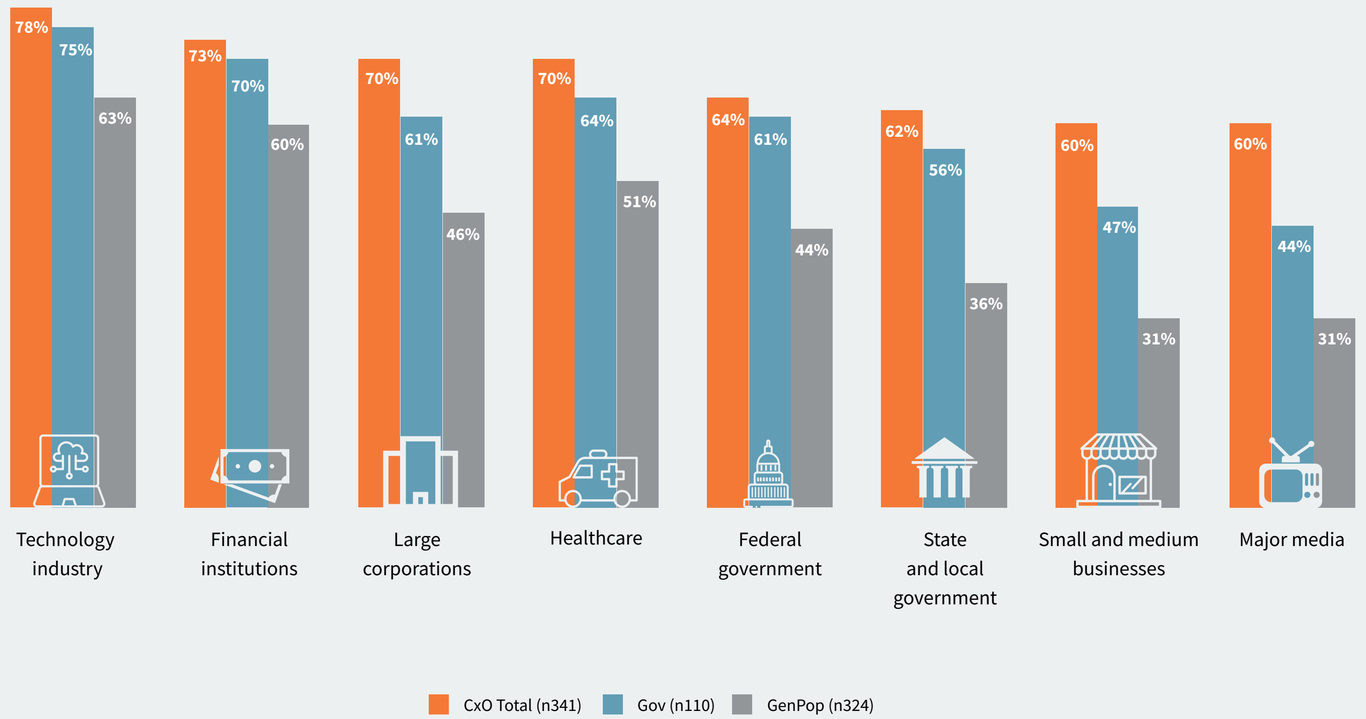
The federal government is among the least trusted by all survey respondents, including the policy makers themselves.

To what extent do you trust the following types of institutions to behave responsibly and in the best interests of the American public as it relates to data security?



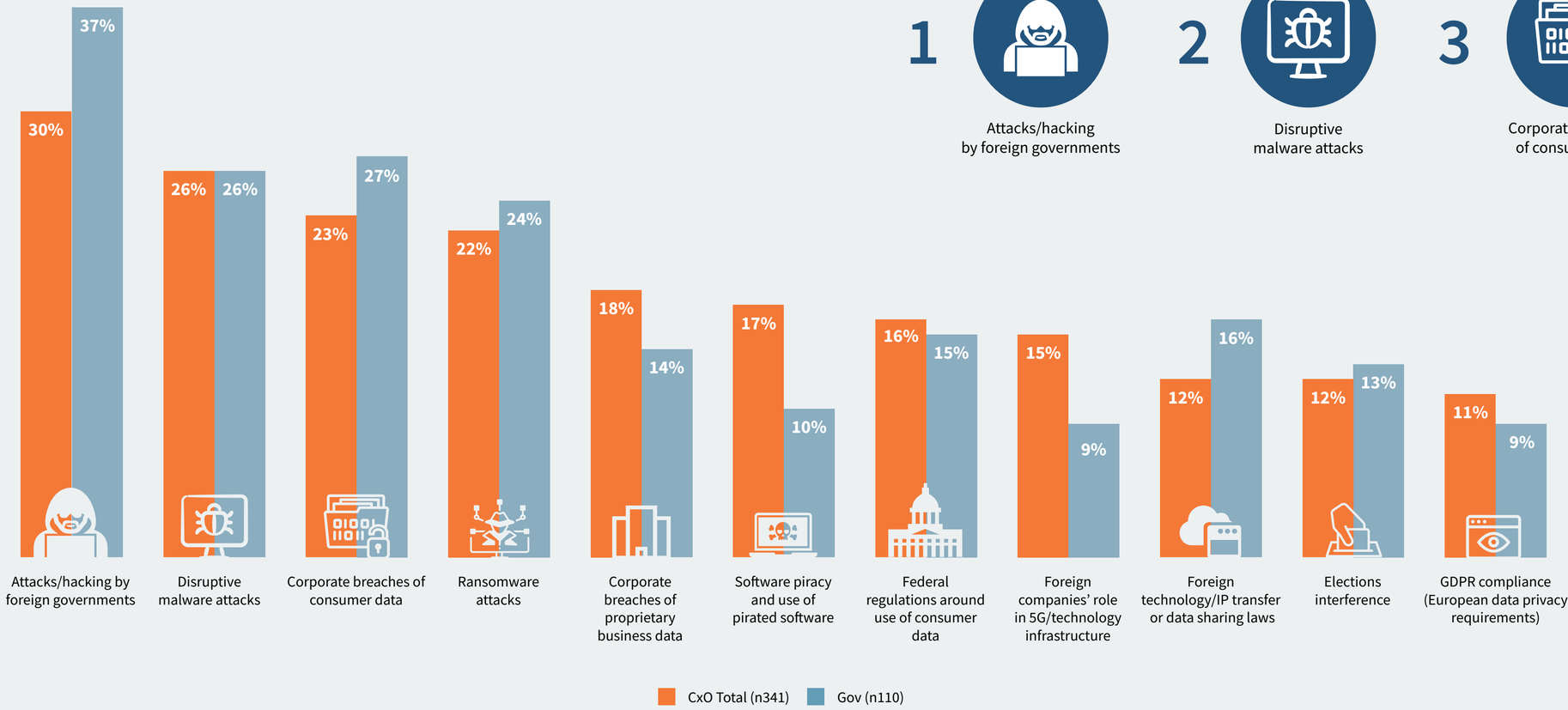
While the majority of the general public trust the technology industry, they are much less trusting of large corporations.

On a scale of 1-5, rate how equipped you feel each of the following is in securing data



Respondents cite foreign governments as the biggest threat facing the technology industry.

Which of the following do you anticipate being the biggest security challenges facing the technology industry?



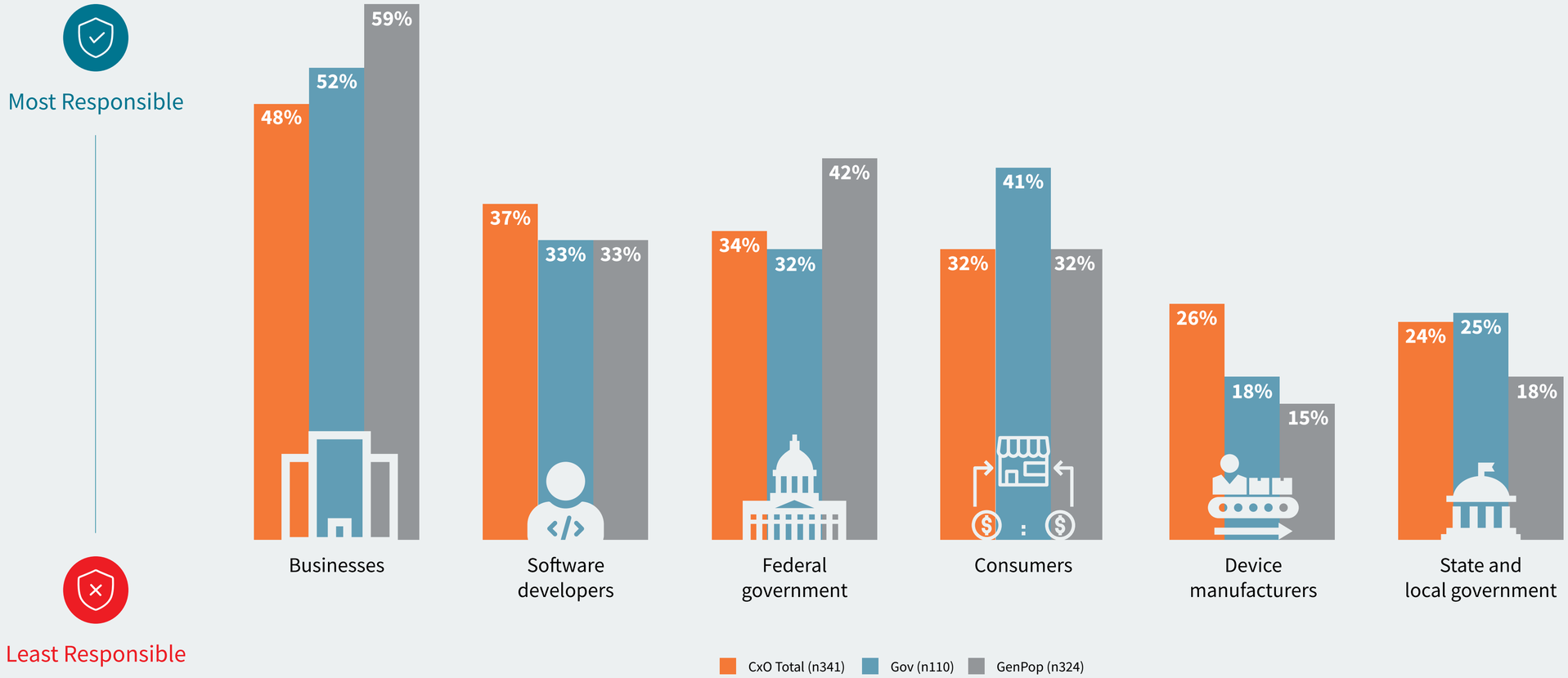
Top 3 security challenges

1. Attacks/hacking by foreign governments
2. Disruptive malware attacks
3. Corporate breaches of consumer data

Who Bears the Responsibility of Data Protection?

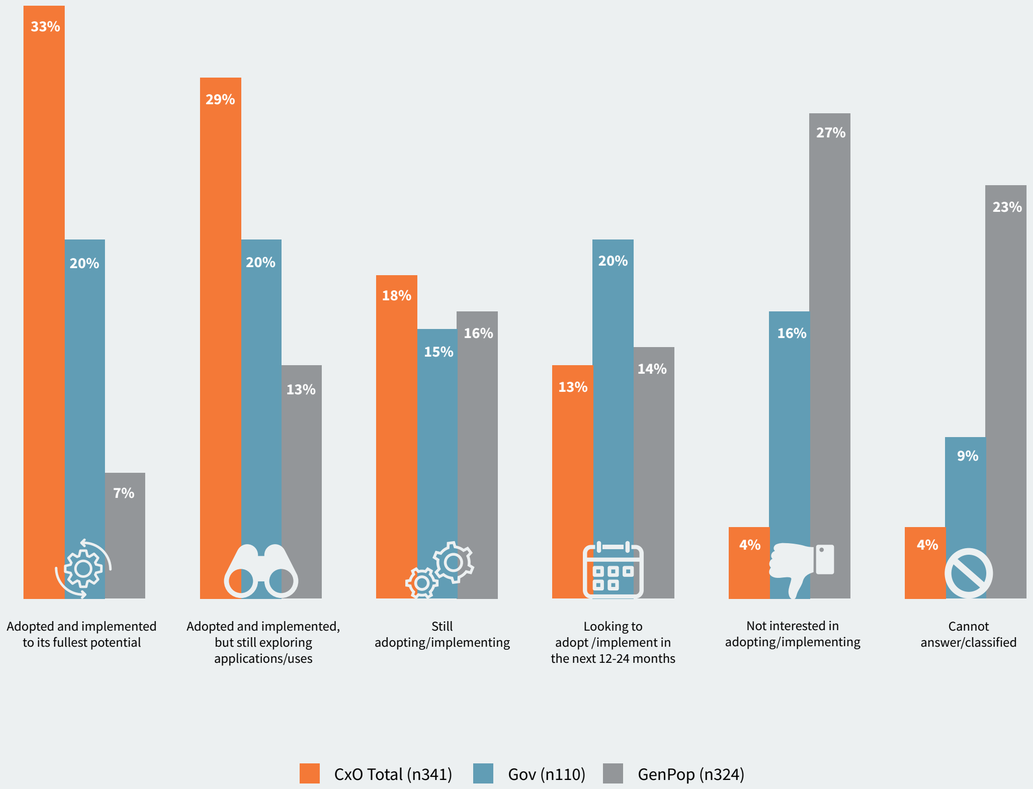
All three respondent groups, including the C-Suite executives themselves, believe that businesses should carry the heaviest burden when it comes to protecting consumer data. Only about **three in ten policy makers** believe the federal government should bear this responsibility.

Who bears the most responsibility for securing consumer information?

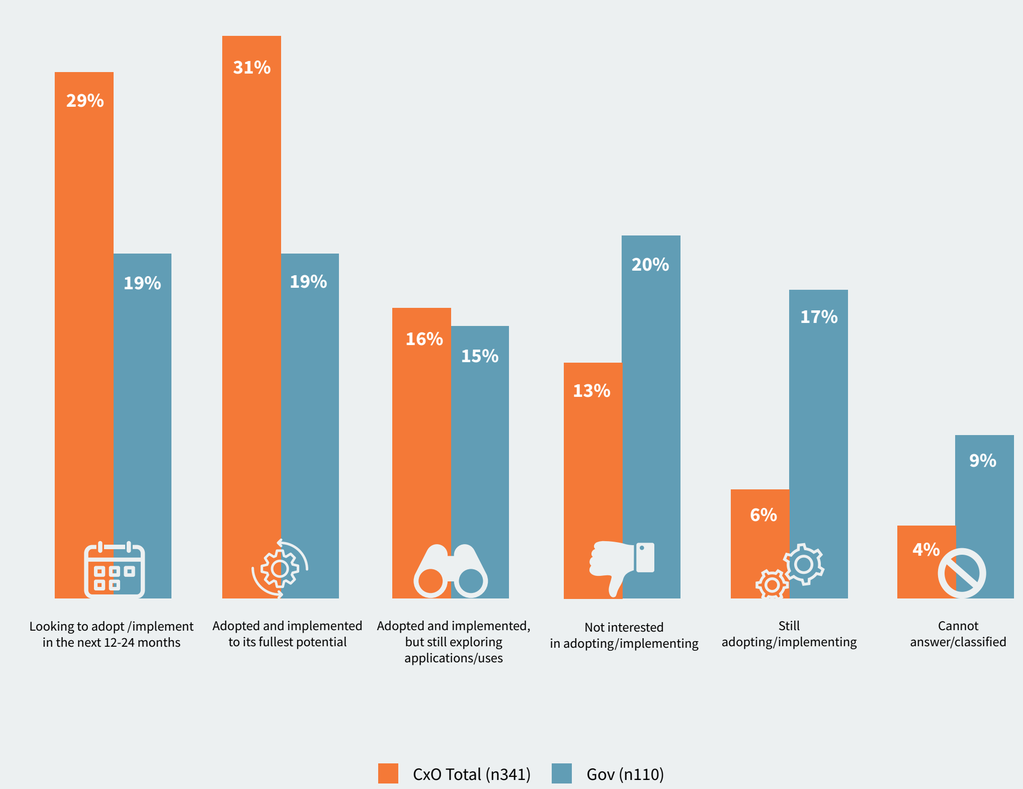


Yet, few companies and policy organizations are adopting the emerging technology that's needed to protect themselves from threats.
80 percent of policy organizations have not implemented AI/ML or autonomous technologies to their fullest potential.

Which of the following best describes your organization's status with respect to AI/ML?



Which of the following best describes your organization's status with respect to autonomous technology?



Autonomous Technology's Impact on the Future

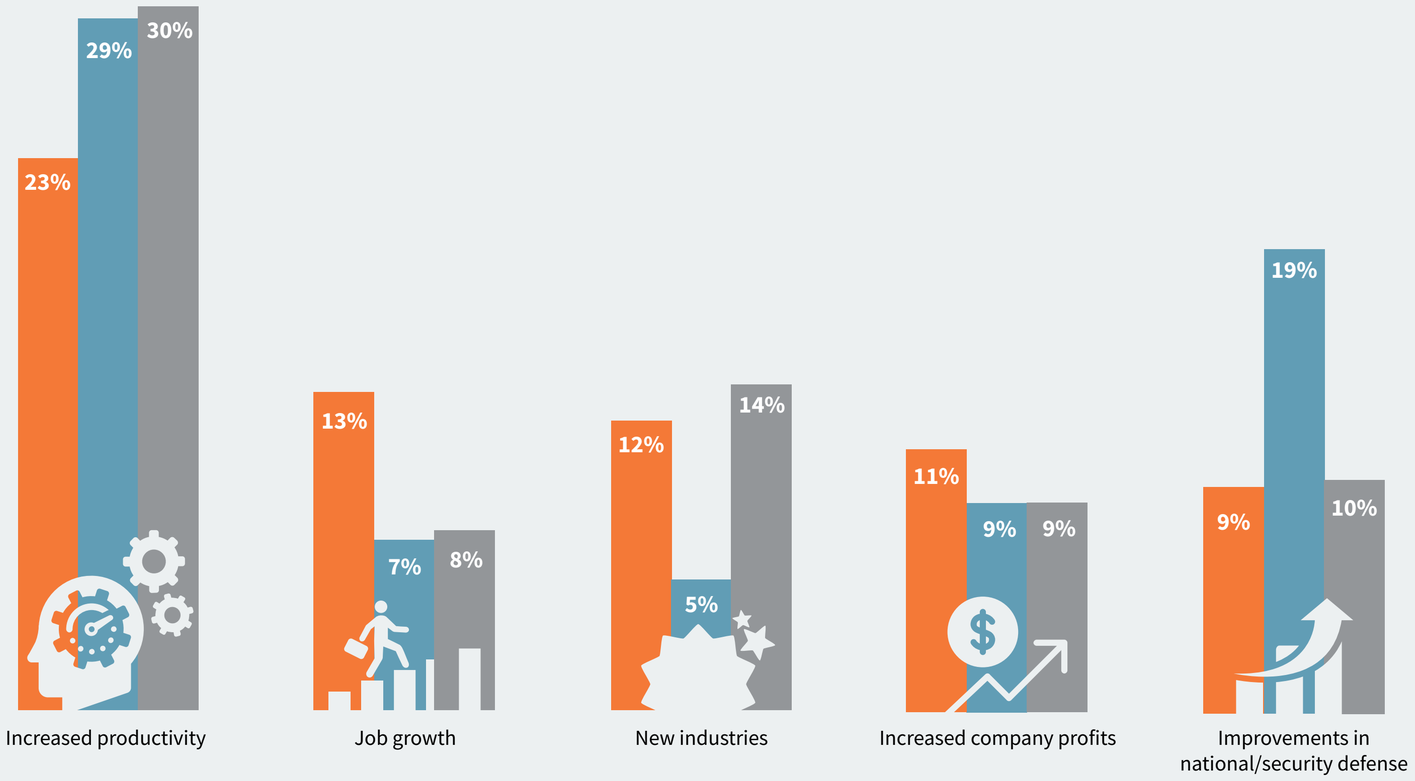
C-Suite executives, policy makers and the general public are in agreement that autonomous technologies – the convergence of AI/ML that delivers self-driving, self-securing, and self-repairing capabilities that can be embedded into a company's core IT infrastructure – will benefit the U.S. economy in the future.

Based on what you have seen, heard, or read about autonomous technologies, which of the following do you believe the most?

	Autonomous technologies will benefit the U.S. economy in the future	Autonomous technologies will hinder the U.S. economy in the future
CxO Total (n341)	88%	12%
Gov (n110)	89%	11%
GenPop (n324)	77%	23%

… with “increased productivity” cited as the top benefit of an autonomous future.

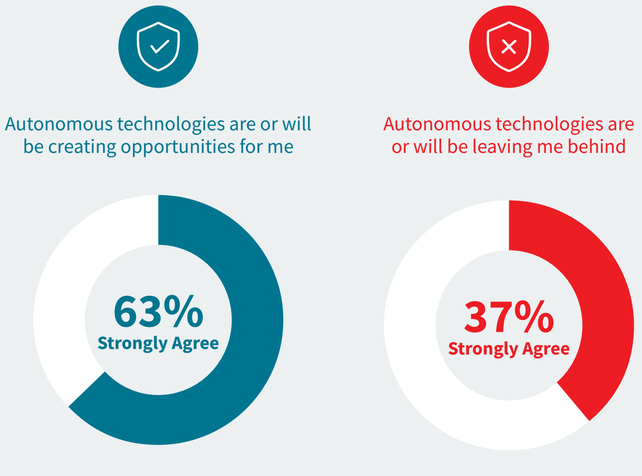
What will be the most significant future benefit of autonomous technologies to the U.S. economy?



Yet, the general public has concerns over autonomous technologies’ impact on their professional lives, with nearly 40 percent believing it will hinder their careers.

Please indicate how strongly you agree or disagree with the following statements:

“Autonomous technologies will help me advance my career.”



GenPop (n324)

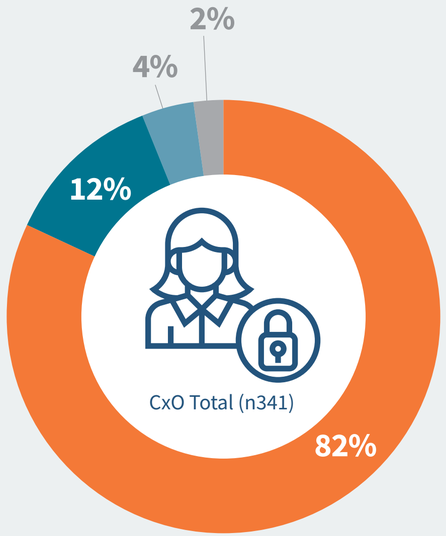
Autonomous Technology's Impact on Security

Autonomous technology is seen as an integral way for companies to protect and handle sensitive information.

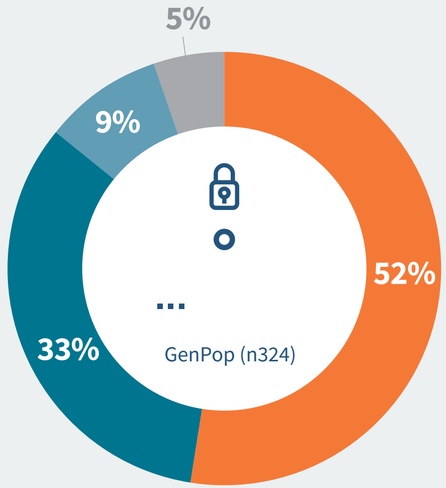
Both C-Suite executives and policy makers strongly believe in the power of autonomous technologies to enhance data protection. In fact, they cite "improved security" as a top benefit of autonomous technologies.

Based on your experience, please indicate how strongly you agree or disagree with the following statement:

"I expect autonomous technologies to improve security and increase trust in the way companies handle my sensitive information."

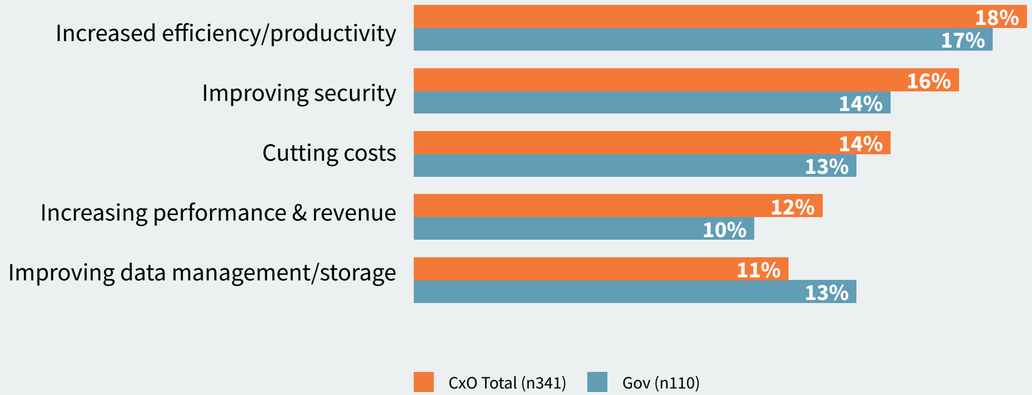


"I expect autonomous technologies to improve security for my company."

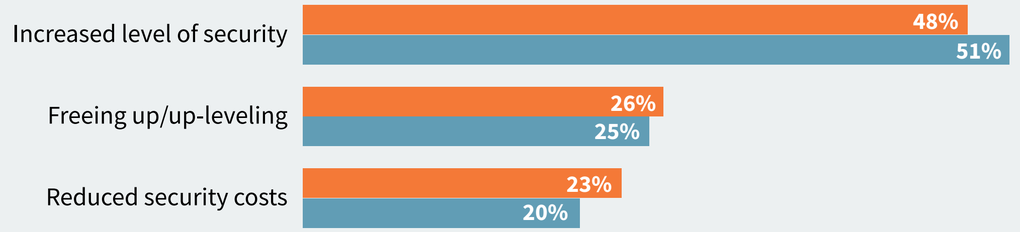


Agree | Neither agree nor disagree | Somewhat disagree | Strongly disagree

Which will be the most significant future benefit of autonomous technologies to companies or organizations?



Which of the following are benefits of having autonomous security?



About the Survey

In Fall 2018, Oracle commissioned technology sector researchers Paradoxes Inc. to field targeted research to understand perceptions of C-Suite decision makers, policy makers and the general public on the current state of U.S. cybersecurity. The survey tool was created by an experienced team of technology and policy researchers, who have been working in this space for over 20 years. It was fielded over January and February of 2019 using a 15 minute-long blind online survey investigating awareness, engagement, corporate and government trust, and current and future plans with technology security practices. The survey tool did not reveal the commissioning company. Respondents to the survey were government policy makers and influencers of various levels located in the U.S. Beltway, enterprise C-Suite executive decision makers – both technology focused and data focused – and an educated and technologically engaged general population. The survey sample consisted of 775 respondents based in the U.S., 341 CxOs (4% margin of error), 110 Government policy influencers (8% margin of error), 324 members of the technologically engaged public (4% margin of error).