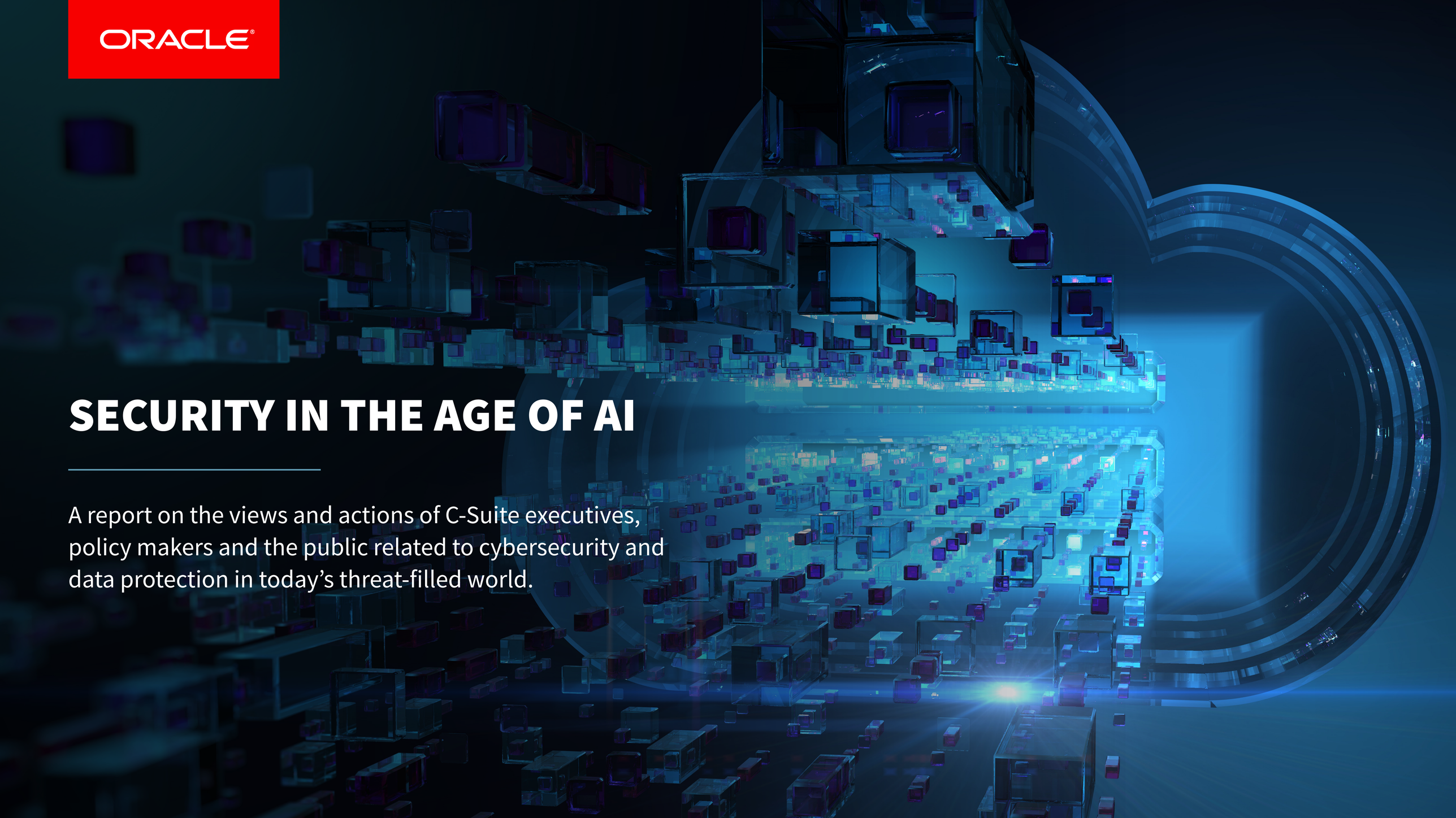
ORACLE

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.



Letter from Edward Screven

I am delighted 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 cyber security.

As confirmed by this survey, data security has become 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 rogue regimes to cybercriminals to hacktivists and insiders. It is estimated that cybercrime will cost the global economy $6 trillion annually by 2021[1].

Adding to this complexity, the current cyber environment is defined by unprecedented connectivity across billions of devices and sensors we rely on every day. The number of internet connected devices is expected to reach nearly 30 billion within the next three years[2] , driven predominantly by the growth in the Internet of Things (IoT) and 5G tech infrastructure advancements. This means more data to store, manage, and secure. It also means more vulnerabilities for attackers to identify and exploit.

Until recently, the cyber threat landscape was tilted in favor of the bad actor, but the rules of the game are beginning to change. 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, but they also free the workforce for more strategic, value-added tasks.

With this survey, we aim to 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 are facing; and the extent to which they are leveraging emerging cloud-based technologies to take their cyber resilience to the next level.

More specifically, we want to understand:

- Confidence in the current state of our cybersecurity
- Views on top security vulnerabilities
- Who is responsible for protecting our data
- Adoption of technology that is now available to combat today's threats

Our nation's security challenges are only mounting. However, thanks to ongoing tech innovation, we have an opportunity to prevail against today's threats. We hope the insights presented in this report will get us one step closer to understanding the threat landscape in which we operate, where the security vulnerabilities lie, and the actions we as business, government and citizens need to take to effectively protect our nation's data.

Sincerely,

Edward Screven
Chief Corporate Architect, Oracle

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

Methodology of Survey

The survey sample consisted of 775 respondents

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 makers 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 adverse 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 of Key Findings

Despite the increasingly dangerous cyber threat landscape, the majority of America's C-suite executives and policy makers are confident in the current state of our cyber security and their ability to manage threats. The general public, however, is much less confident.

- The majority of C-suite executives and policy makers said they have confidence in current levels of data security within U.S. businesses, government and consumer data.
- However, **only one third of the general public have confidence in data security** within U.S. businesses and government.
- Despite public skepticism, **82 percent of C-suite executives and 78 percent of policy makers believe that their organization's information is secure**.

While both C-suite executives and policy makers rank "human error" as the top cybersecurity risk for their organization, they choose to invest in people (via training and hiring) instead of the cloud-based technology, such as Artificial Intelligence (AI) and Machine Learning (ML), that has 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 ranked the lowest.
- **80 percent of policy makers and nearly 70 percent of C-Suite executives have not adopted and/or implemented AI to its fullest potential.**
- Yet, when asked, they admit that these same cloud-based technologies are critical to improving their cybersecurity defenses.

Next to small businesses, C-Suite executives and policy makers trust the technology industry most when it comes to responsibly protecting America's data.

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

Respondents believe foreign governments pose a bigger threat to the technology industry, more than ransomware attacks, piracy and twice as concerning as election interference.

Nearly forty 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.
- After businesses, policy makers believe the responsibility to secure consumer data lies with the consumers themselves.

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

- Autonomous technologies built on AI and machine learning deliver the most advanced data protection through self-driving, self-securing, and self-repairing capabilities that minimize human error. 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 **(83 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.

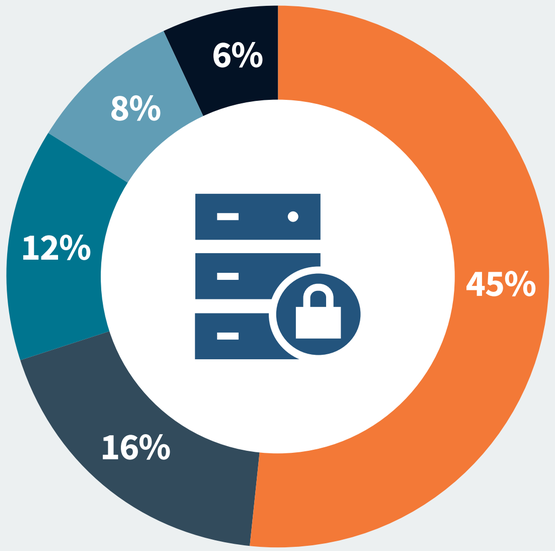
A majority of the respondents believe autonomous technologies will benefit the U.S. economy, with "increased productivity" cited as the top benefit. Yet, the general public has mixed feelings about the technology's impact on their professional lives.

- 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**. Yet, at an individual level, nearly two thirds don't believe autonomous technologies will help advance their careers.
- Additionally, around **40 percent of the general public feel that autonomous technologies will leave them behind**, as opposed to creating opportunities for them.

Securing Data Is Now Policy Makers' Top Priority

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

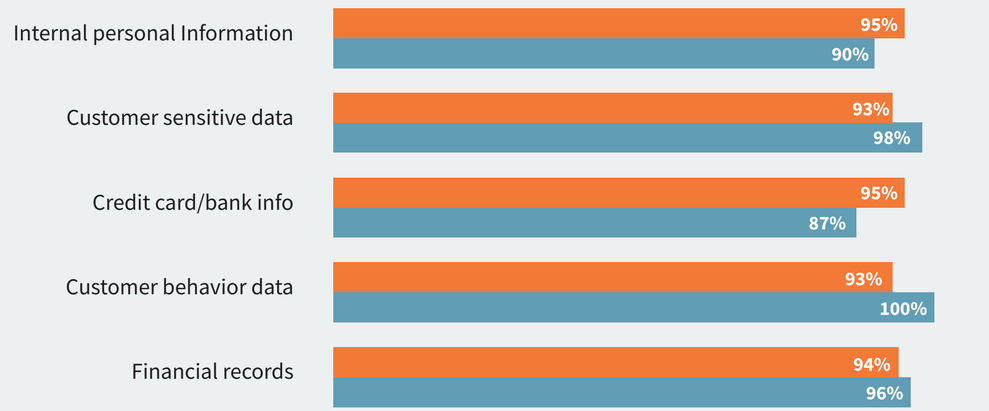
Thinking back on everything that you have read, heard, seen over the last 12 months, which of the following is the biggest concern for your organization over the next 12-24 months?



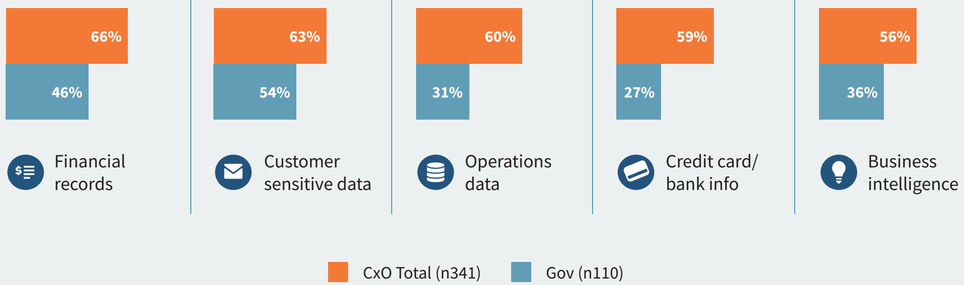
- Data security
- Adoption/implementation of technology solutions
- Efficiency/productivity
- Keeping/acquiring talent
- Controlling costs

The data that companies and policy makers have within their walls has never been more critical to their success…

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

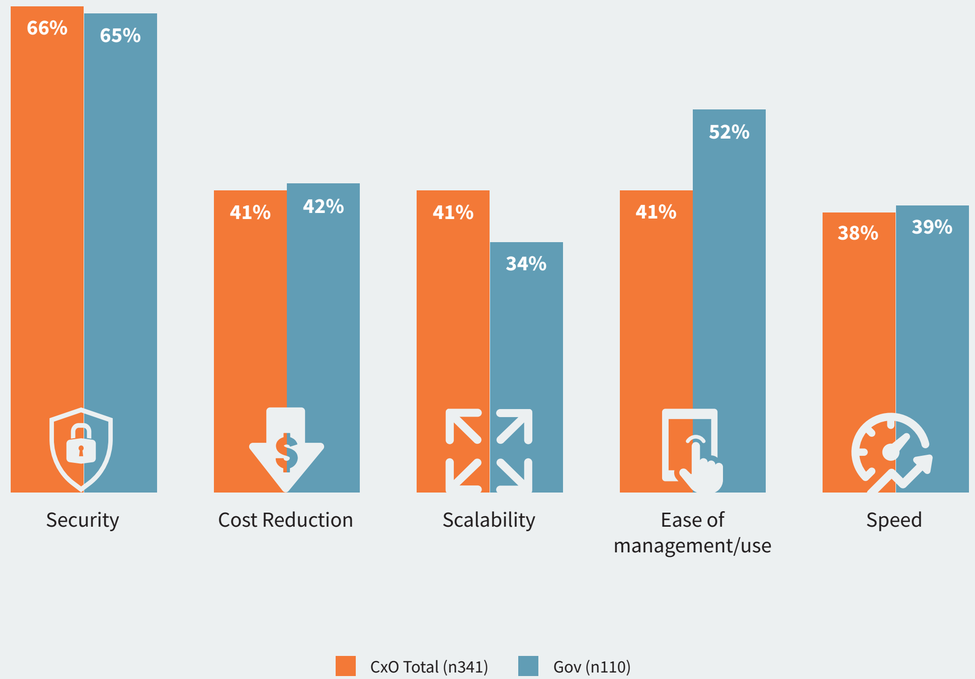


Which of the following types of sensitive information do you use and store at your business?



…and more than **6 in 10 C-suite executives and policy maker respondents** cite security as the top benefit of cloud technology.

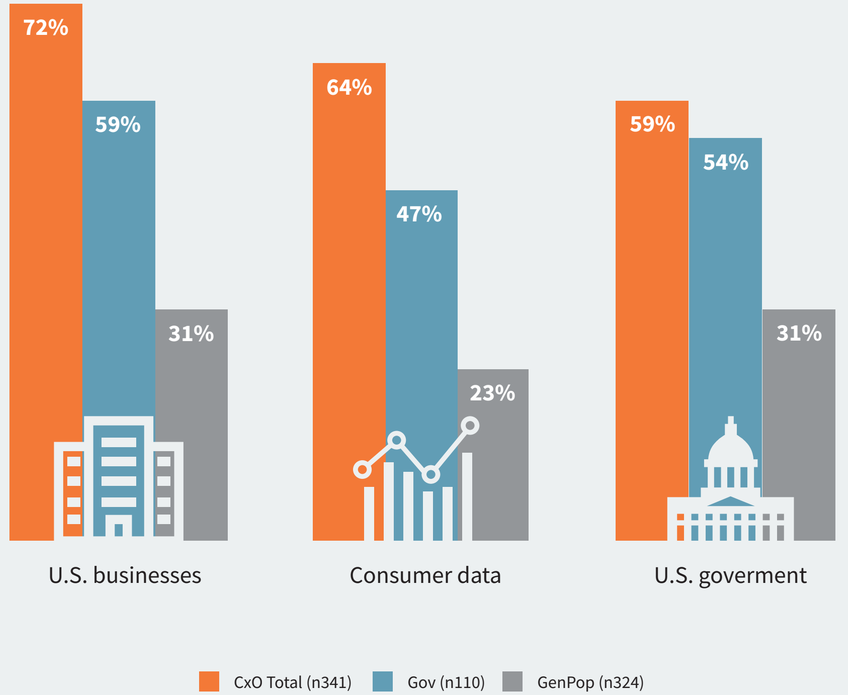
What are the biggest benefits of cloud computing for your organization today?



‘All is Well’ When It Comes to Security, Say C-Suite and Policy Makers

The reality is a majority of Americans have been personally impacted by a major data breach[1]. Despite the fact that there have been nearly 10,000 data breaches since 2005, exposing over 1.5 billion records[2] , the majority of America’s C-suite executives and policy makers are confident in the state of our data security. The general public, however, is far more skeptical.

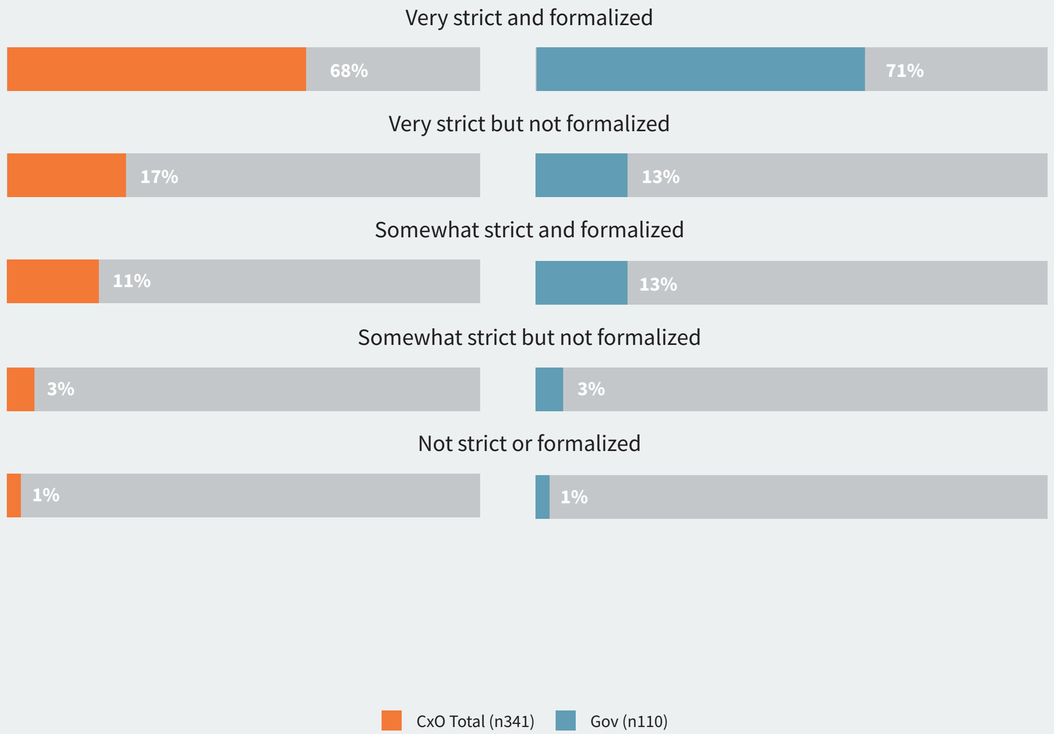
On a scale of 1-5, rate your confidence of the current data security within:



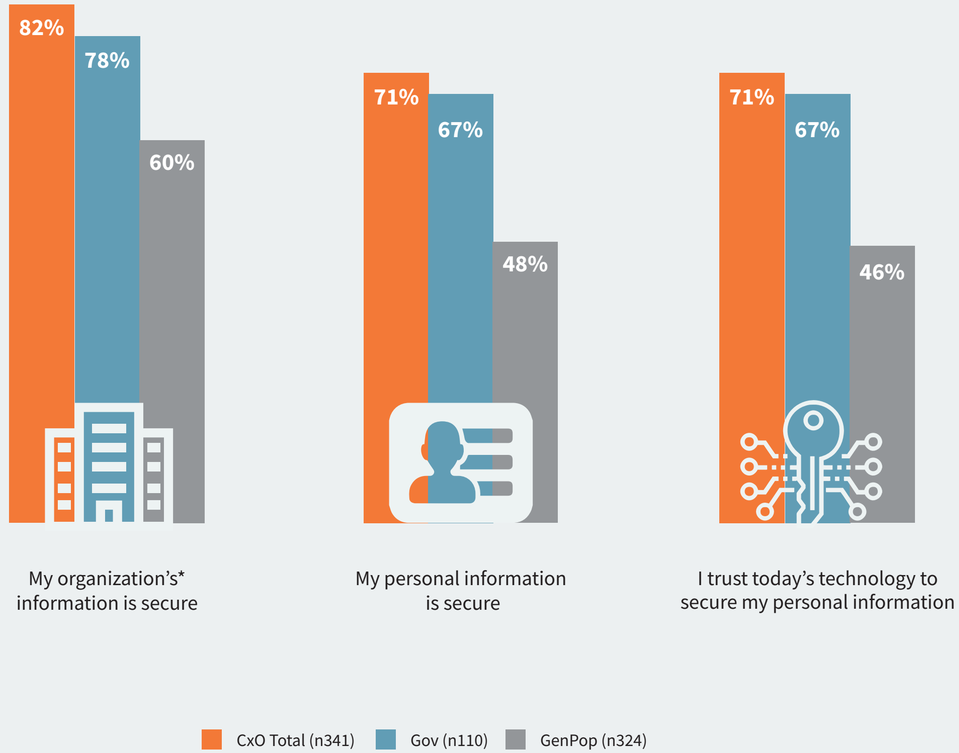
[1]Pew Research: Americans and Cybersecurity: https://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/
[2]Identity Theft Resource Center 2019 Data Breaches: https://www.idtheftcenter.org/data-breaches/

They also believe their current policies around data security are more than adequate to keep sensitive information secure…

Which of the following best describes your company's policies around security?



Please indicate your level of agreement with each of the following statements.

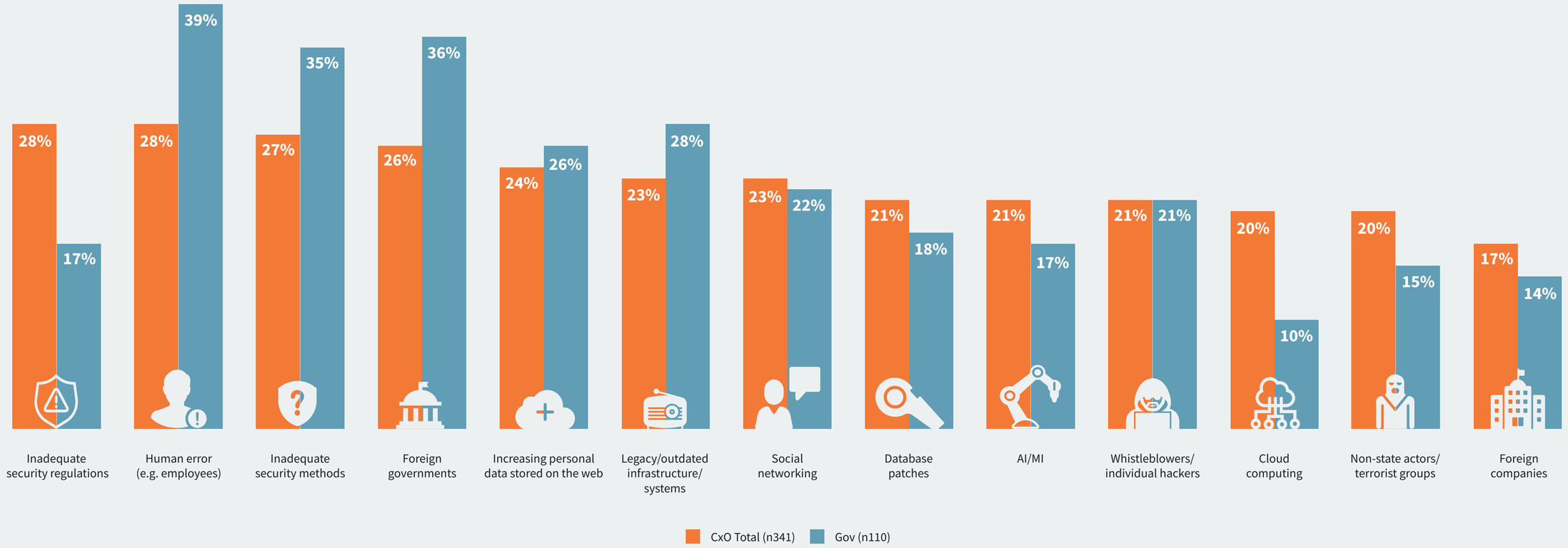


*For general population, "organization" refers to the employer of the respondent at the time of the survey.

‘People’ Seen as Biggest Security Vulnerability, Yet C-Suite and Policy Makers Will Continue to Invest in People over Tech to Solve Security Issues

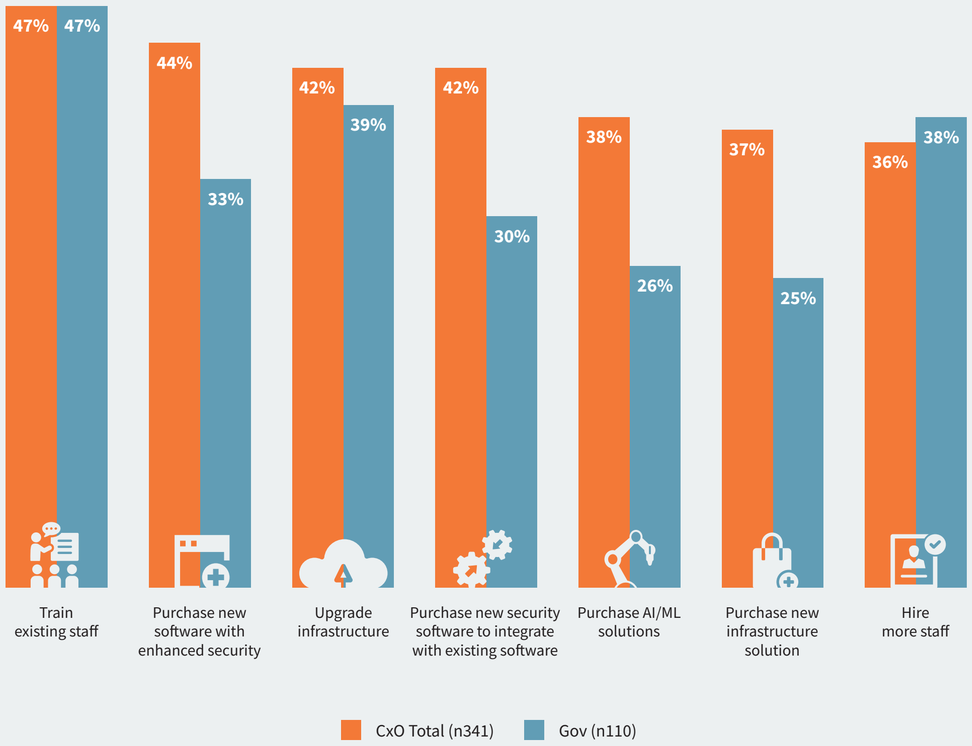
When asked about security vulnerabilities, employees are seen as the biggest risk in our cybersecurity defenses across America, according to both C-Suite executives and policy makers…

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

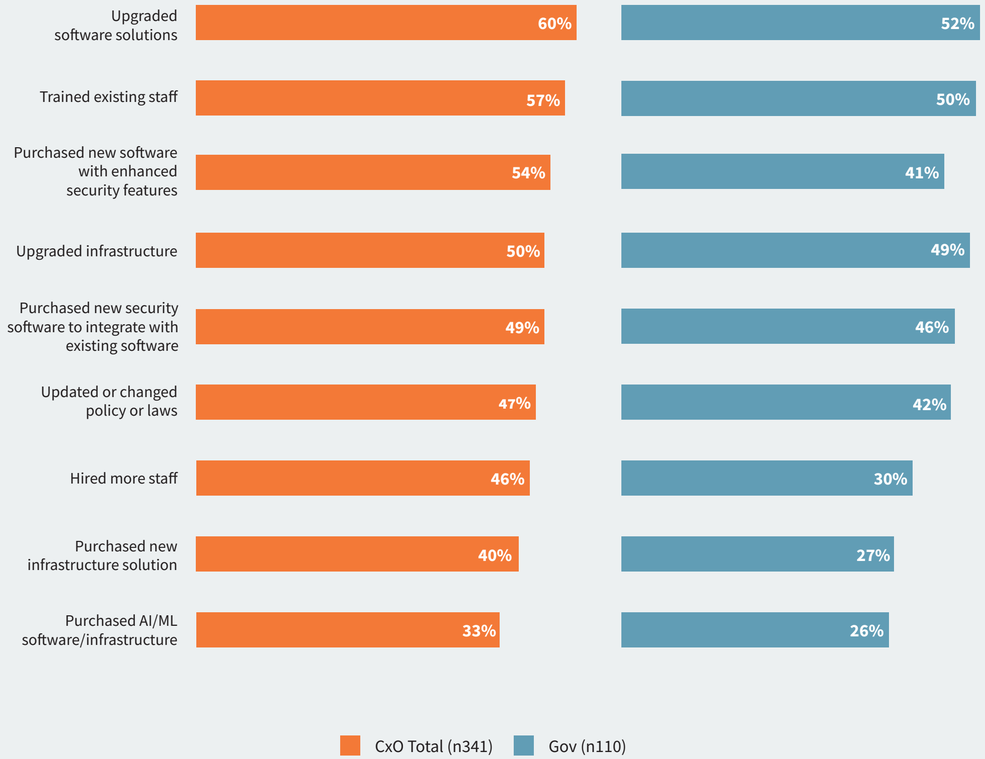


While people are seen as the biggest security risk, far too few companies and organizations invest in the emerging cloud-based technology advancements that minimize human error by leveraging the power of AI and ML to automatically detect and respond to security threats before they take place. In fact, they're investing more in humans – which they cite as the source of their vulnerability.

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

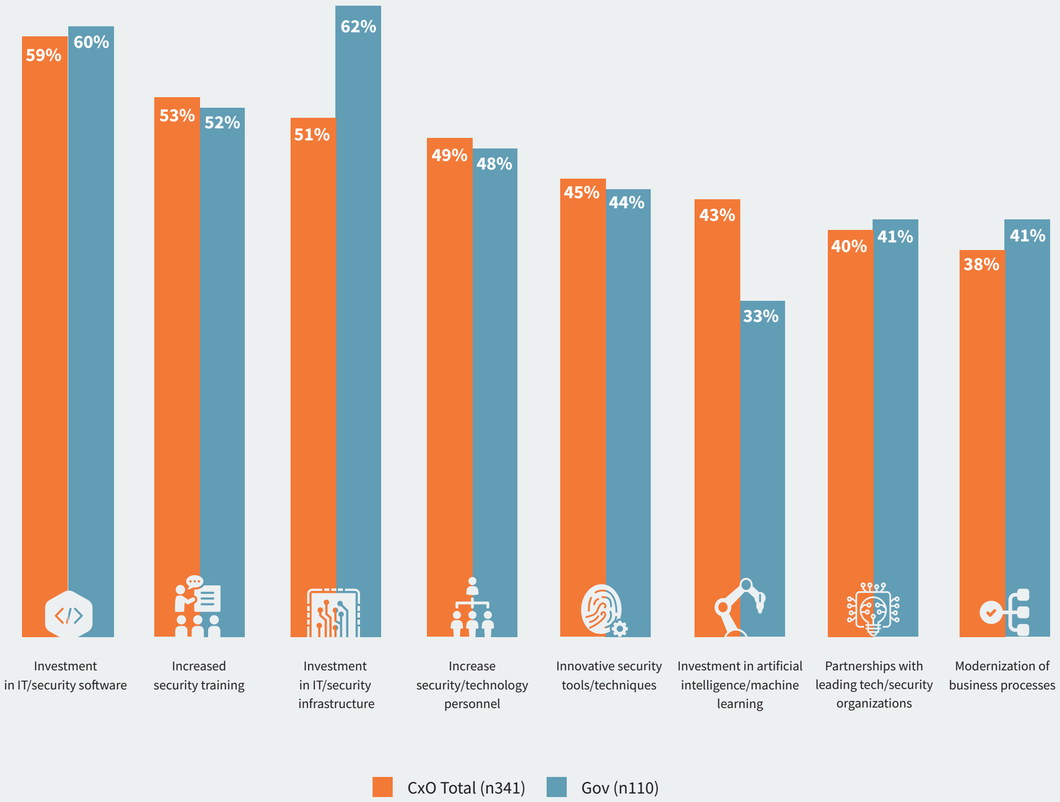


Which of the following has your organization done in the past 5 years to improve security?



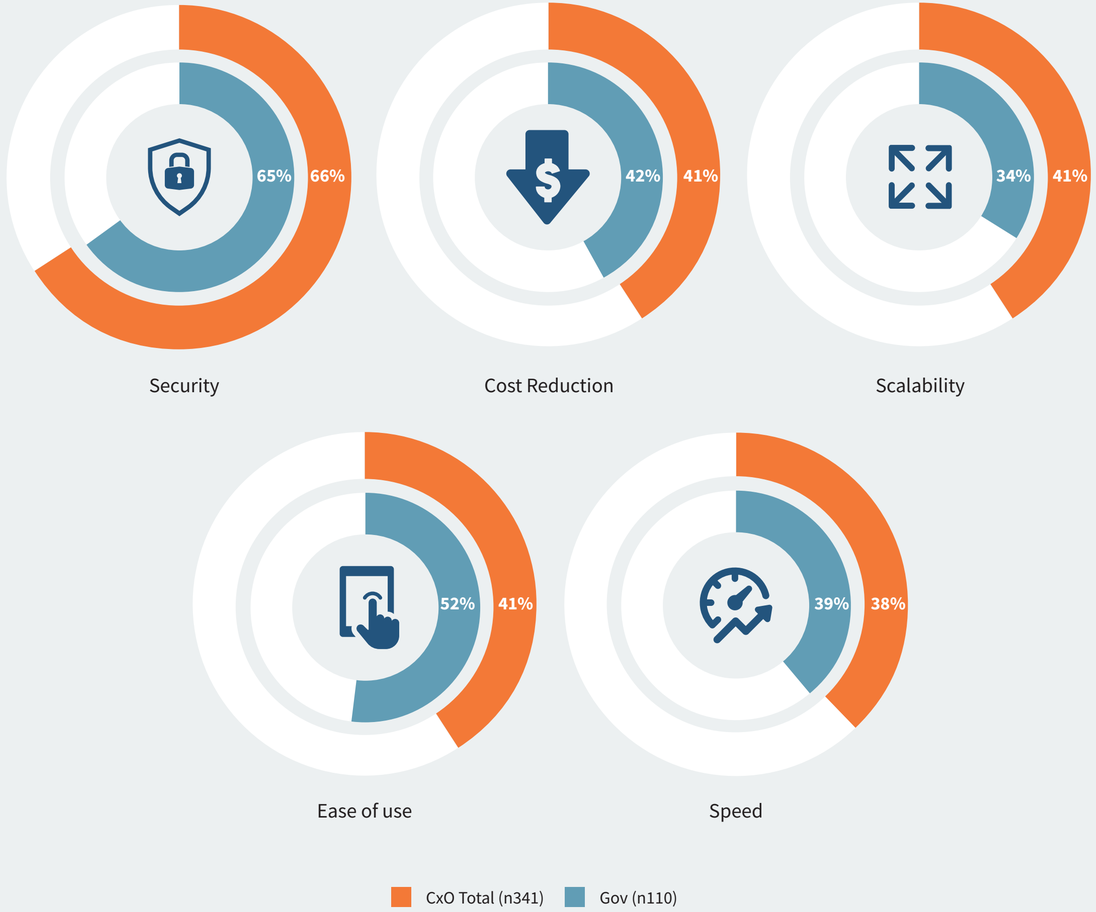
Yet, when asked what the U.S. government needed to keep our country's data safe from attackers, **6 in 10 respondents** admit that investing in these same emerging cloud-based technologies are paramount…

Which of the following would make the US 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?



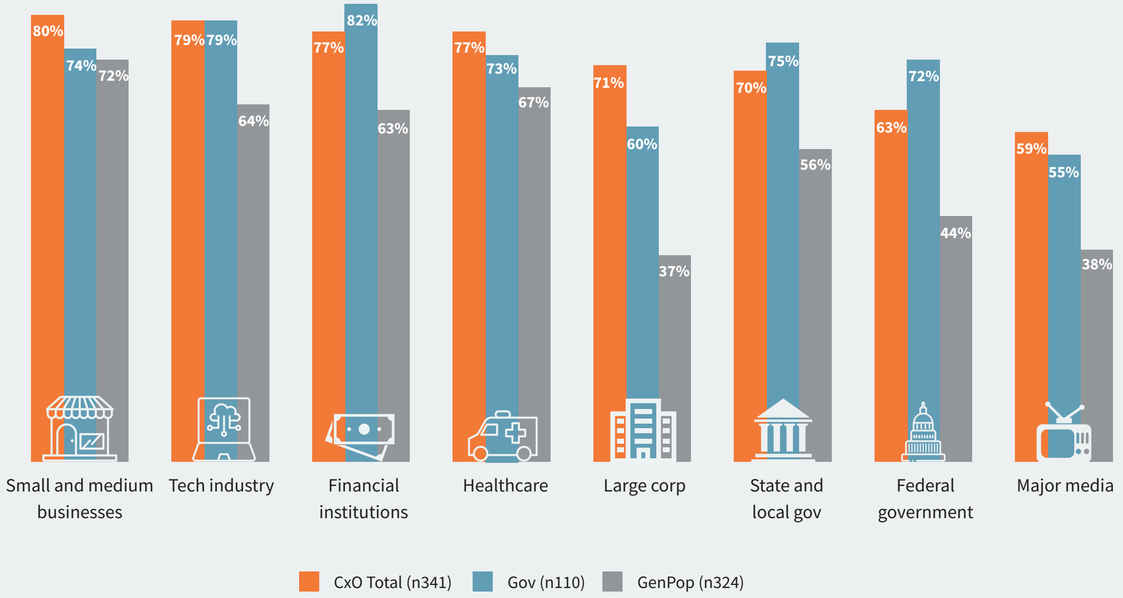
Trust in Organizations' Ability to Protect Data

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

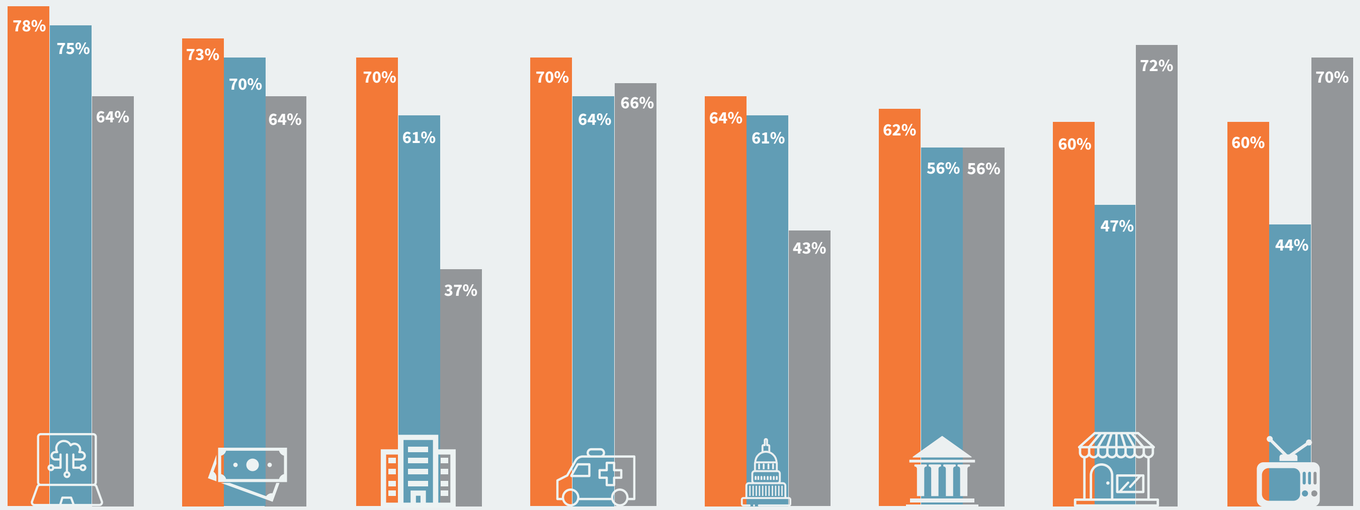
While the majority of the general public trust the technology industry, they are much less trusting of large corporations.

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?



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

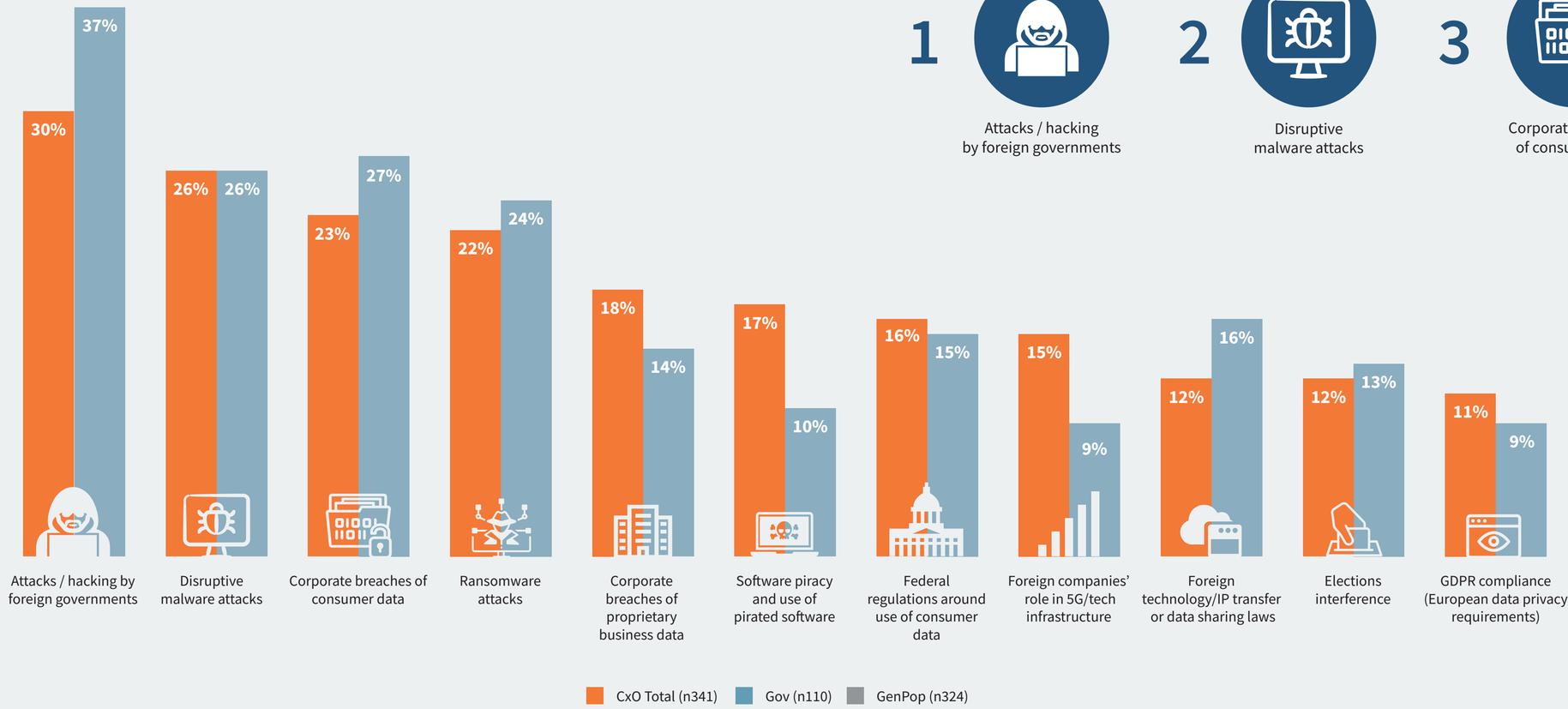


Rank the top five companies you distrust the most in the tech industry to keep your sensitive information safe?

1. Facebook
2. Twitter
3. Alibaba
4. Amazon
5. Apple

Respondents cite foreign governments as the biggest threat facing the technology industry, larger than ransomware attacks, piracy and twice as concerning as election interference.

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



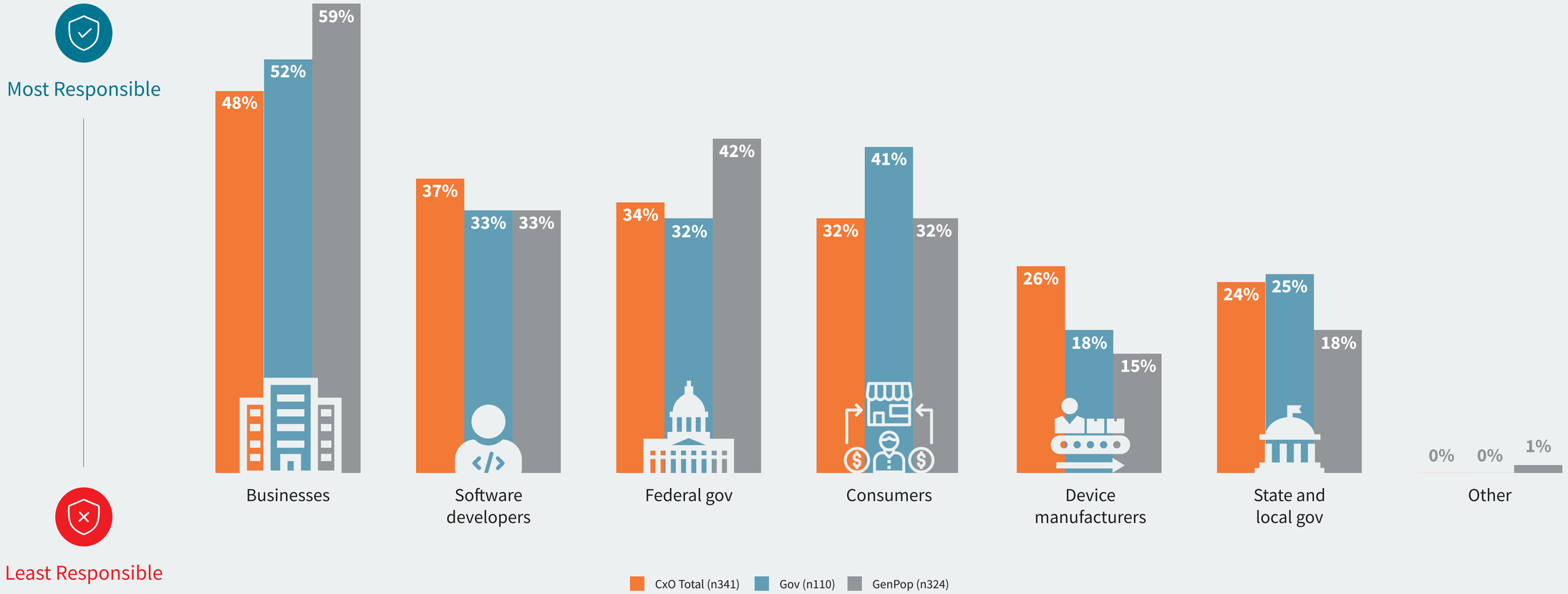
Top 3 security challenges

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

Who Bears the Responsibility of Data Protection?

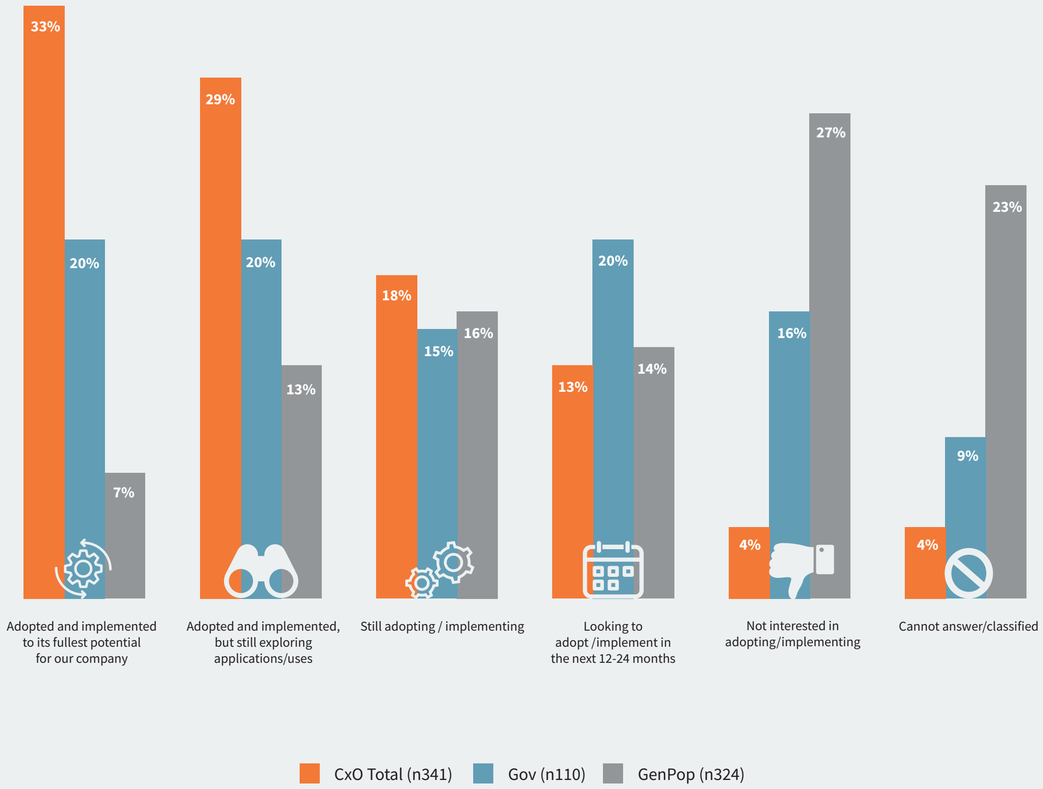
All three respondent groups, including the C-suite executives themselves, believe that businesses should carry the heaviest burden when it comes to protecting consumer data. Interestingly, only about **3 in 10 policy makers** believe the federal government should bear this responsibility.

Who bears the most responsibility for securing consumer information?

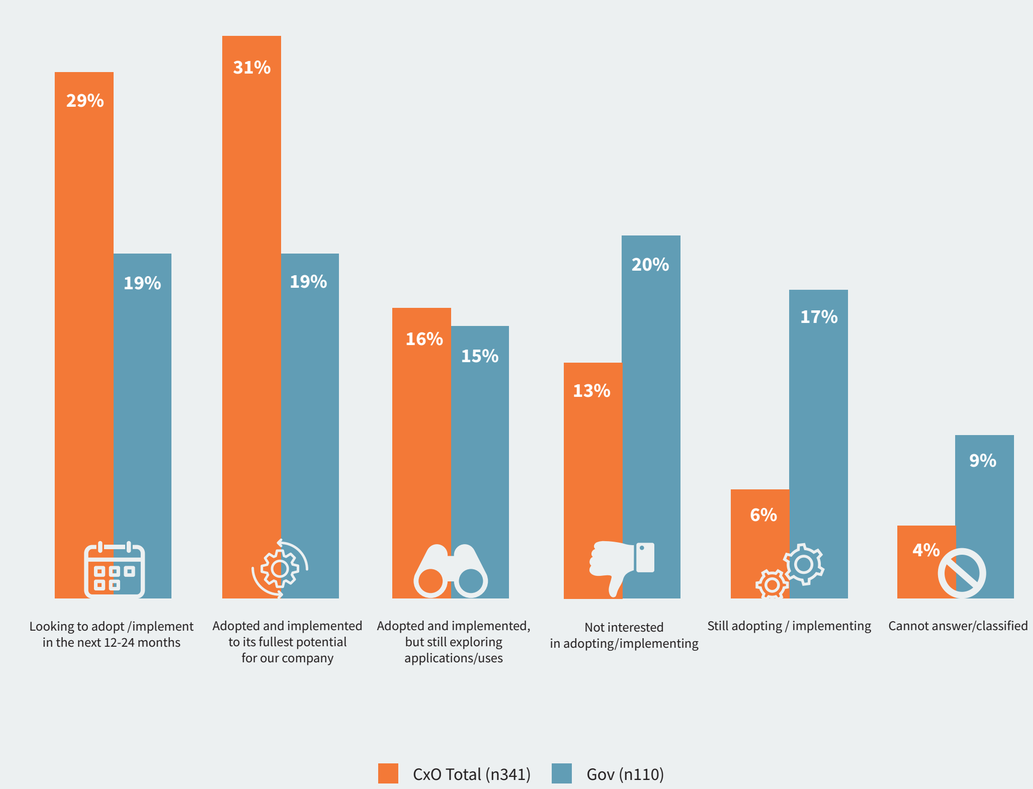


Yet, far too few companies and policy organizations are adopting the emerging tech that's needed to protect them from threats.
A staggering 80% of policy organizations have not implemented AI/ML or autonomous technologies to its fullest potential.

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?

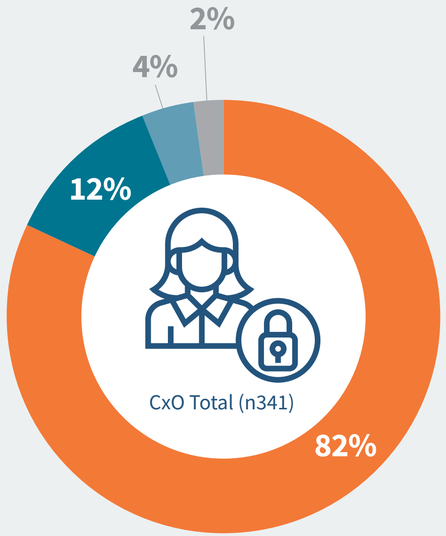


Autonomous Technology's Impact on Security

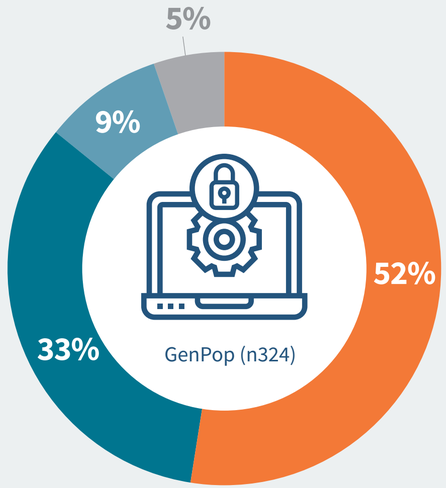
Autonomous technology – the convergence of Artificial Intelligence and Machine Learning that delivers self-driving, self-securing, and self-repairing capabilities that can be embedded into a company's core IT infrastructure – is seen as an integral way for companies to protect and handle sensitive information.

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."



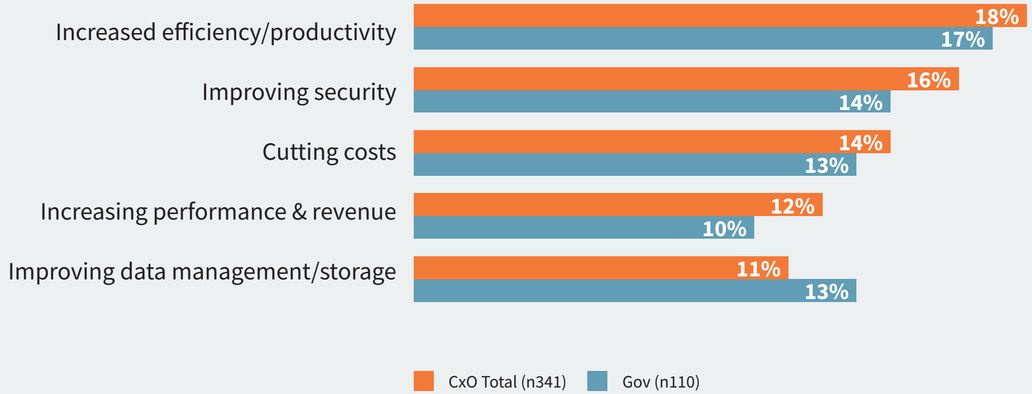
"I expect autonomous technologies to improve security for my company."



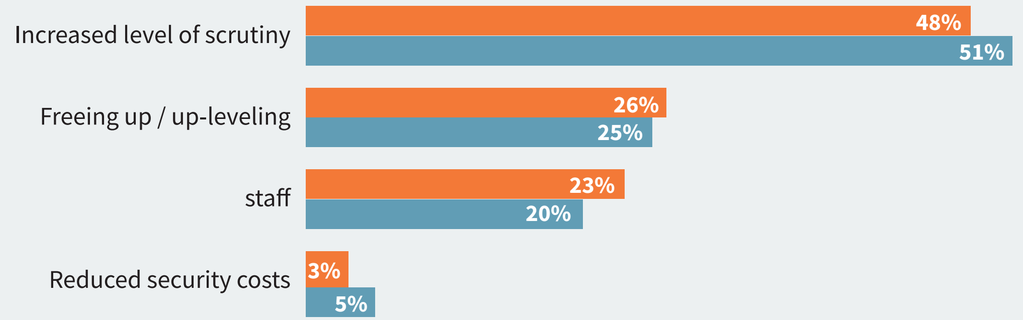
Agree | Neither agree nor disagree | Somewhat disagree | Strongly disagree

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

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



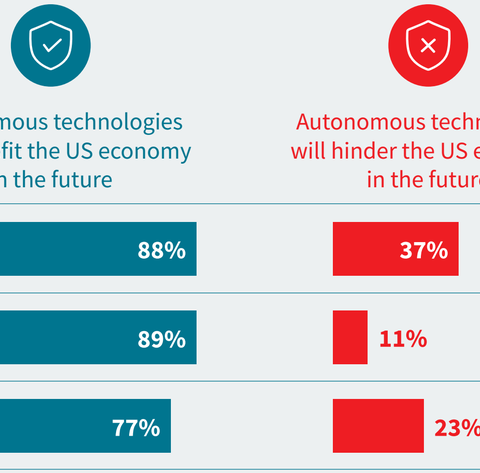
Which of the following are benefits of having autonomous security?



Autonomous Technology's Impact on the Future

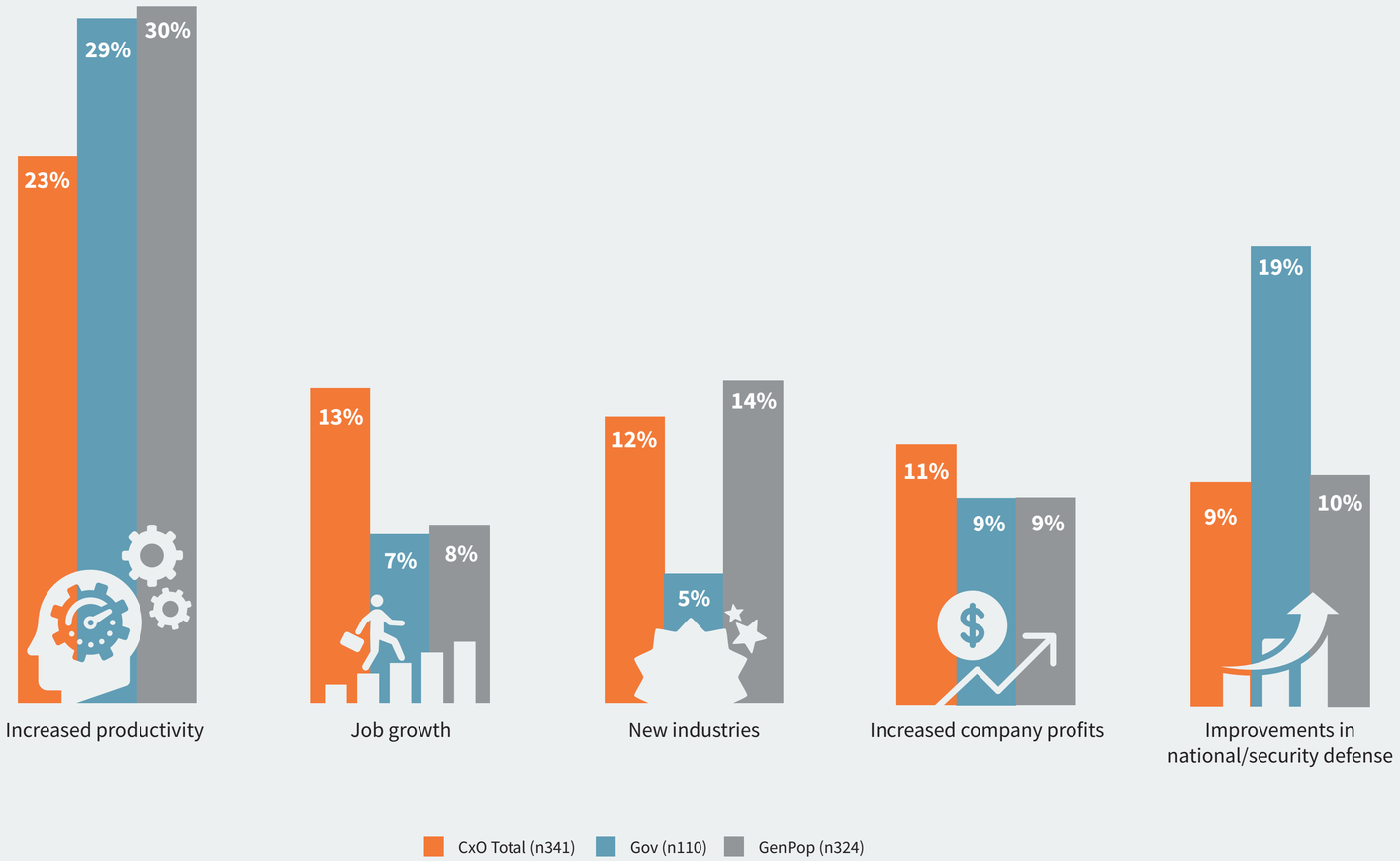
C-suite executives, policy makers and the general public are in agreement that autonomous technologies will benefit the U.S. economy in the future…

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



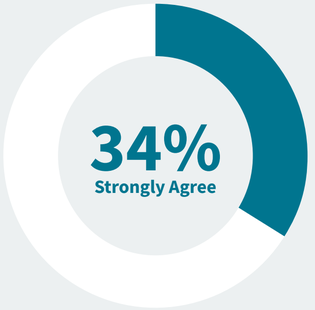
… with “increased productivity” cited as the top benefit of an autonomous future.

What will be the most significant future benefit of autonomous technologies to the US economy?



Yet, the general public has concerns over autonomous technologies’ impact on their professional lives, with a majority 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?



Autonomous technologies are or will be creating opportunities for me

Autonomous technologies are or will be leaving me behind

Conclusion

- The general public does not see eye to eye with C-suite executives and policy makers on data security. The general population has much less confidence in the current state of data security than C-suite executives or policy makers.
- A similar discrepancy exists vis-a-vis the general public's level of trust in large corporations to responsibly protect America's data. C-suite executives and policy makers trust large corporations more than the general public does when it comes to data security.
- Human error is seen as the top cybersecurity vulnerability across the board. Yet, instead of capitalizing on newly emerging cloud-based technology advancements that can minimize human error and boost data protection through Artificial Intelligence and Machine Learning, both C-suite executives and policy makers continue to invest in people – the source of their vulnerability – to face cyber threats.
- Respondents assign the responsibility of data protection to business. Yet, only a small fraction of companies are adopting the emerging technology that's needed to effectively fulfill this role.
- While C-suite executives and policy makers have not adopted AI and autonomous technologies to their fullest potential, they are confident in the ability of these technologies to significantly improve the way we secure data. Both audiences cite "security" as one of the biggest future benefits of autonomous technologies.
- There is general consensus among the survey respondents that autonomous technologies will positively impact the U.S. economy in the future, with "increased productivity" seen as the most significant future benefit. However, the general public is more skeptical when it comes to autonomous technologies' impact on their individual careers.