Clearwater

FIRST ANNUAL GENERATIVE AI STUDY:

Healthcare Edition

iSMG

TABLE OF CONTENTS

Welcome Summary.. 3

Introduction... 4

Welcome Summary.. 3

About the Sponsor.. 4

Survey Results... 5

Conclusions 23

Expert Analysis 24

Summarizing the Healthcare Edition

Within the broader generative AI survey across multiple vertical sectors, responses from within the medical sector were broken out to see if there were any differences in approach. While the results of the smaller sample are less robust, they are nonetheless indicative of trends.

ABOUT THE SPONSOR

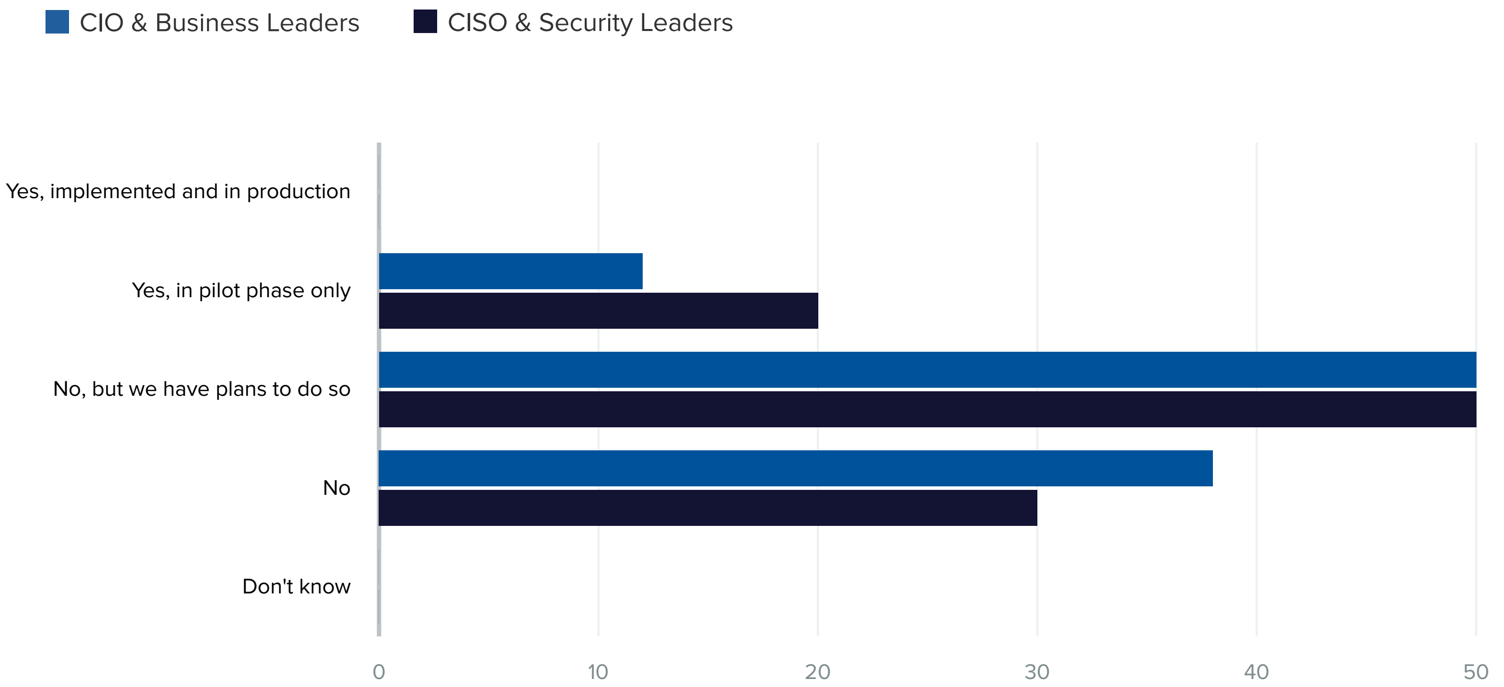
Clearwater

Clearwater helps organizations across the healthcare ecosystem move to a more secure, compliant, and resilient state so they can achieve their mission. The company provides a deep pool of experts across a broad range of cybersecurity, privacy, and compliance domains, purpose-built software that enables efficient identification and management of cybersecurity and compliance risks, and a tech-enabled, 24/7 Security Operations Center with managed threat detection and response capabilities.

For more information, visit:
clearwatersecurity.com

SURVEY RESULTS

1. Does your company currently use generative AI?

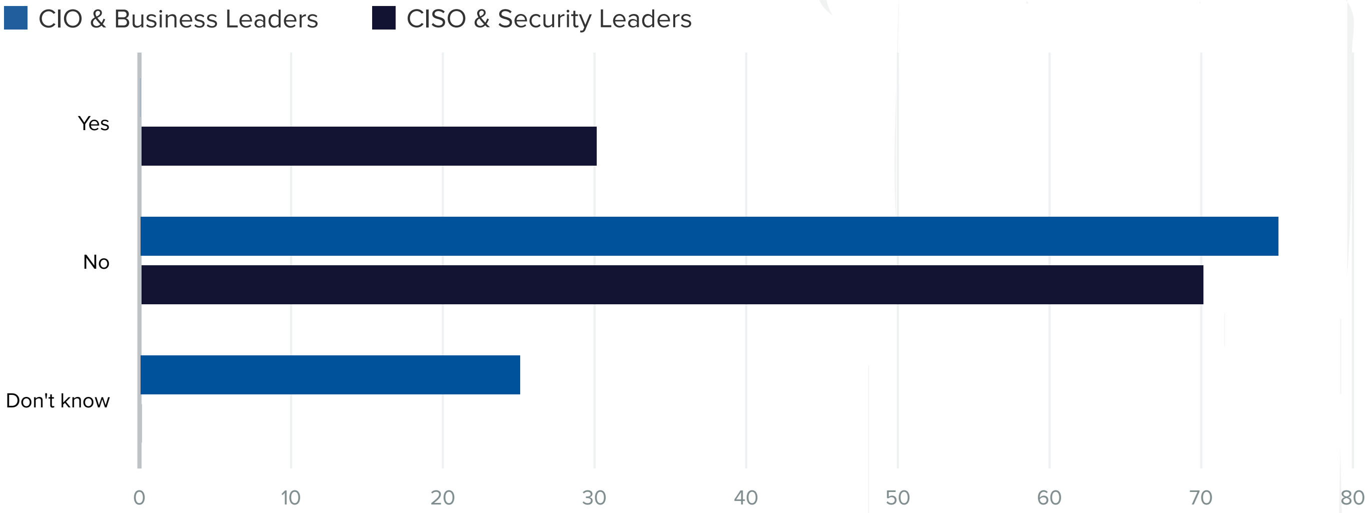


None of the medical respondents have AI implemented and in production, compared to 15% in the wider cohort, but 12% of business leaders and 20% of cybersecurity leaders are trialing it in a pilot phase. Fifty percent of both groups have plans to use AI, and 38% of business leaders and 30% of cybersecurity leaders have no plans to do so.

This contrasts with the broader group across multiple verticals, where business leaders are between 5% and 10% more likely than cybersecurity professionals to report implementation of AI and cybersecurity leaders are more likely to have no plans to implement AI, at 34% compared to 19% for business leaders, thus the opposite of the medical sector.

Combining business leader and cybersecurity leader results from the health sector, the results are none with AI implemented, compared to 15% across all verticals; 17% in pilot phases, compared to 28%; 50% with plans for implementation, compared to 27% across all verticals; and 33% with no plans to use AI, compared to 27% across all verticals.

2. Does your organization allow staff to use generative AI for work purposes on their own initiative?



While 30% of cybersecurity leaders say this is allowed, none of the business leaders say that it is. Seventy-five percent of business leaders say it is not allowed, as do 70% of cybersecurity leaders. The remaining 25% of business leaders say they do not know, whereas none of the cybersecurity leaders say they do not know.

Again, this is a reversal of the situation for respondents across all verticals, where 63% of business leaders report that AI use is allowed, compared to 47% of cybersecurity professionals. It suggests that there is a wider disconnect between business leaders and cybersecurity professionals within the health sector.

3. Who in your organization is responsible for deploying generative AI productivity solutions (job title)?

Most business leaders say the CIO is responsible. They also mention the board, CFO and IT – but not the CISO. Cybersecurity professionals mostly say the CTO is responsible but also mention the CISO, CIO and IT or say that no such role exists.

These responses are broadly in line with other vertical sectors.

4. Who in your organization is responsible for securing generative AI productivity solutions (job title)?

Most business leaders say the CIO is responsible, but CFO and CISO are also mentioned. The cybersecurity professionals are almost unanimous in citing the CISO. There appears to be a disconnect between who each group thinks is responsible. Across other verticals, CISO is the title most mentioned by business leaders.

5. Who in your organization will be responsible for ongoing management of generative AI productivity solutions (job title)?

Business leaders again select CIO. They mention CFO and IT. Cybersecurity leaders also say CIO but include CISOs as well as IT, strategy and ops.

6. Which of the generative AI tools/platforms do you use or are you aware of?

Business leaders only mention ChatGPT, and cybersecurity professionals say ChatGPT, Bard, GitOps, Azure AI and CybrSec. Obviously, this is a smaller sample than the wider cohort, but across all vertical, a much wider range of alternatives are mentioned. This likely reflects the current lack of implementation and pilots compared to other sectors. It also reflects healthcare being behind other sectors in implementing AI.

7. What are the main productivity gains you get/envision your organization getting from use of generative AI?

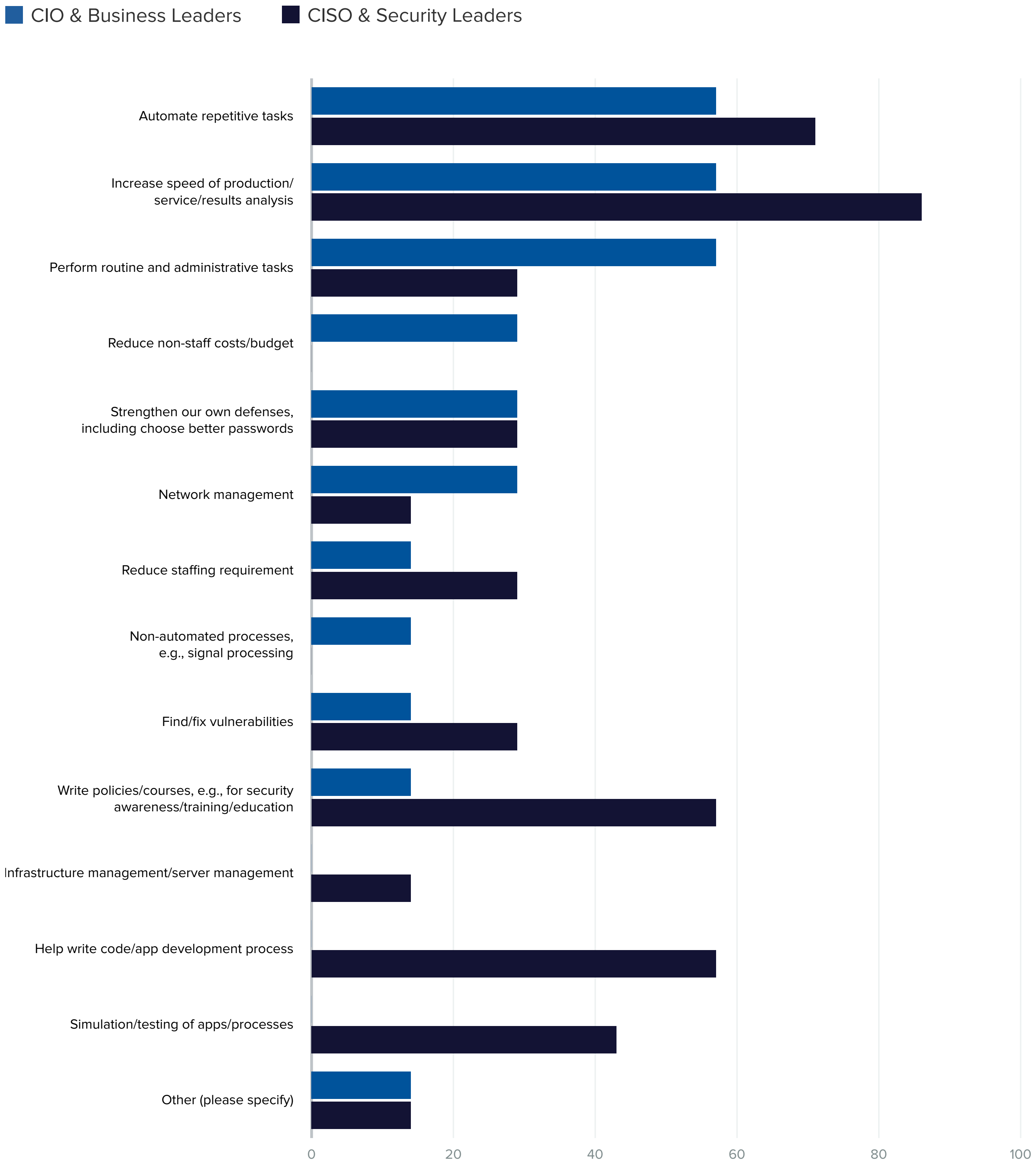
For cybersecurity professionals, increasing the speed of production/service/results analysis leads the list at 86% followed by automation at 71%. These two benefits are also tied for first place among business managers, at 57%, along with performing routine and administrative tasks, which 29% of cybersecurity leaders choose. In third place for cybersecurity professionals is writing policies/courses, at 57%. Simulation testing is at 43% for cybersecurity professionals and zero for business leaders.

Much of the divergence here is due to the different roles of each group, but it is likely that this will spill over into perceptions of what AI is for and how it is used in the organization as a whole.

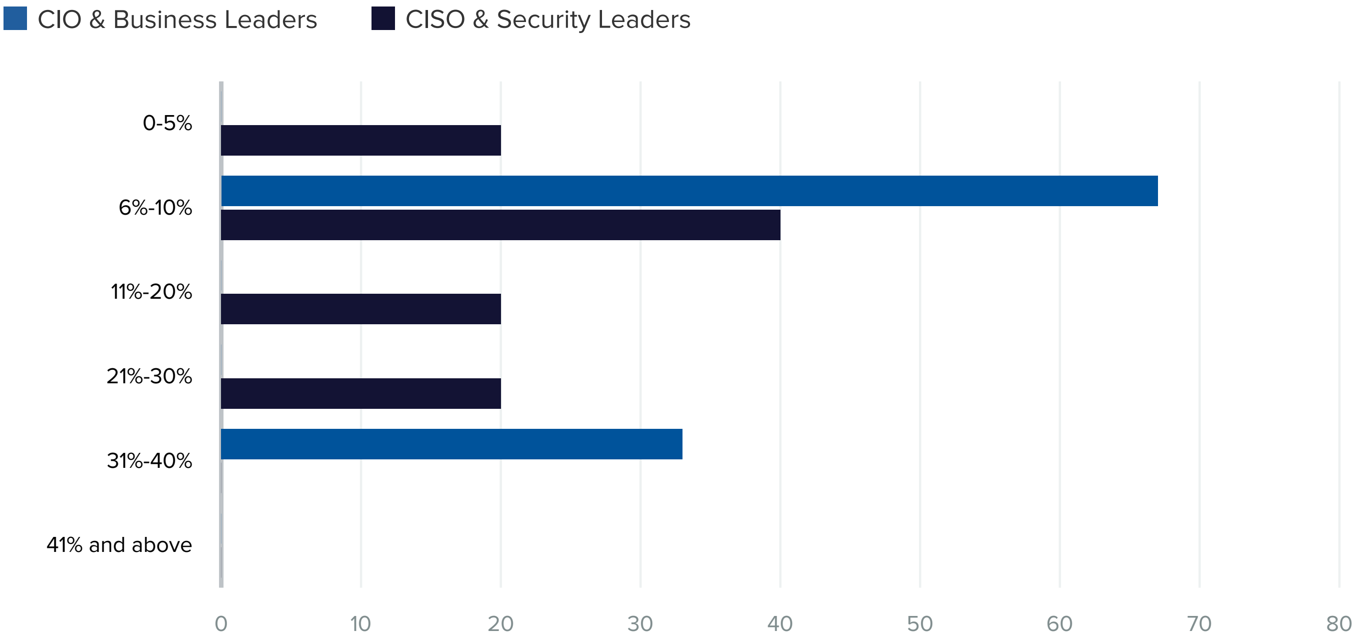
Across all verticals, the leading response is automating repetitive tasks, at 67% for business leaders, 58% of cybersecurity leaders and 62% for all respondents. This is followed by increasing the speed of production/service/results analysis at 65% and 52%, respectively, and 59% overall. Performing routine and administrative tasks comes in third at 58% and 45%, respectively, and 52% overall.

FULL CHART ON NEXT PAGE

CHART 7


CIO & Business Leaders
CISO & Security Leaders
Automate repetitive tasks
Increase speed of production/ service/results analysis
Perform routine and administrative tasks
Reduce non-staff costs/budget
Strengthen our own defenses, including choose better passwords
Network management
Reduce staffing requirement
Non-automated processes, e.g., signal processing
Find/fix vulnerabilities
Write policies/courses, e.g., for security awareness/training/education
Infrastructure management/server management
Help write code/app development process
Simulation/testing of apps/processes
Other (please specify)
0
20
40
60
80
100

8. If you currently use AI systems, what productivity gains do you estimate you achieve compared to the systems they replace?



Sixty-seven percent of business leaders and 40% of cybersecurity professionals anticipate gains of 6% to 10%, and 20% of cybersecurity professionals expect gains of 0 to 5% compared to none of the business leaders seeing such a low return. Thirty-three percent of business leaders anticipate a gain of 31% to 40% compared to none of the cybersecurity leaders seeing that return.

The higher expectation of gains by business leaders is in line with the findings of the wider cohort.

9. For what use cases/ environments do you use/ envision your organization using generative AI?

Marketing: One hundred percent of business leaders intend to use AI for this. Among cybersecurity leaders, 17% currently use it and the remainder intend to use it.

Customer service/remote patient services - including via chatbots: One hundred percent of cybersecurity leaders intend to use AI for this. Among business leaders, 33% use it and the remainder intend to use it.

Legal/regulatory compliance: One hundred percent of business leaders intend to use AI for this. Among cybersecurity leaders, 25% currently use it and the remainder intend to use it.

Enterprise Knowledge management: One hundred percent of both groups intend to use AI for this.

Software development: One hundred percent of cybersecurity leaders intend to use AI for this. Business leaders did not say they use it or intend to use it.

Fraud: One hundred percent of both groups intend to use AI for this.

AML: One hundred percent of cybersecurity leaders intend to use AI for this. Business leaders did not say they use it or intend to use it.

Cybersecurity, from threat detection to incident response: Fifty percent of business leaders intend to use AI for this, and 50% already do. Among cybersecurity leaders, 20% currently use it and the remainder intend to use it.

Document automation/Customer/Patient data processing: One hundred percent of business leaders intend to use AI for this. Among cybersecurity leaders, 25% currently use it and the remainder intend to use it.

Foundation technology/infrastructure - vector databases, LLM orchestration, growth in large language models/training vs. inferencing cost and infrastructure, LLM operations: One hundred percent of cybersecurity leaders intend to use AI for this. Business leaders did not say they use it or intend to use it.

Production: One hundred percent of both groups intend to use AI for this.

Medical diagnosis and treatment: One hundred percent of both groups intend to use AI for this.

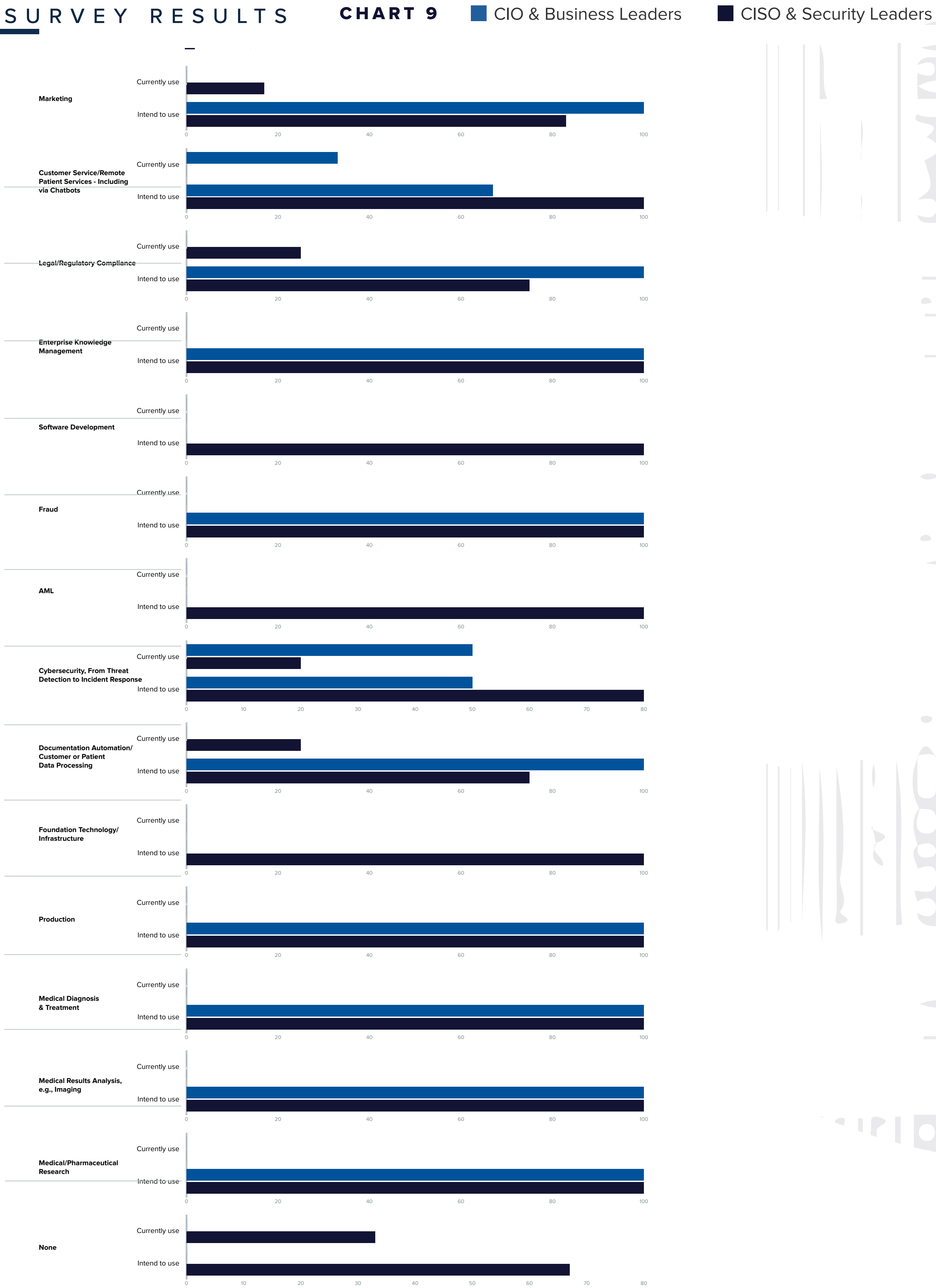
Medical results analysis, e.g. imaging: One hundred percent of both groups intend to use AI for this.

Medical/pharmaceutical research: One hundred percent of both groups intend to use AI for this.

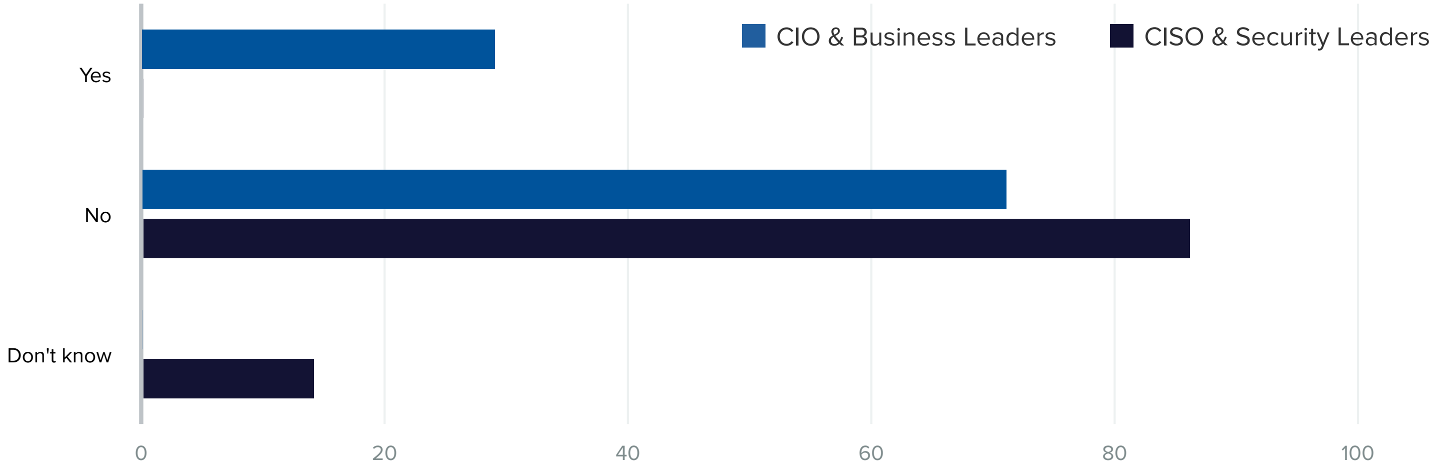
While the expectation of using AI for medical applications is high, the sector is behind others in implementation.

FULL CHART ON NEXT PAGE

CHART 9


■ CIO & Business Leaders
■ CISO & Security Leaders
Marketing
Currently use
Intend to use
Customer Service/Remote Patient Services - Including via Chatbots
Currently use
Intend to use
Legal/Regulatory Compliance
Currently use
Intend to use
Enterprise Knowledge Management
Currently use
Intend to use
Software Development
Currently use
Intend to use
Fraud
Currently use
Intend to use
AML
Currently use
Intend to use
Cybersecurity, From Threat Detection to Incident Response
Currently use
Intend to use
0
10
20
30
40
50
60
70
80
Documentation Automation/ Customer or Patient Data Processing
Currently use
Intend to use
Foundation Technology/ Infrastructure
Currently use
Intend to use
Production
Currently use
Intend to use
Medical Diagnosis & Treatment
Currently use
Intend to use
Medical Results Analysis, e.g., Imaging
Currently use
Intend to use
Medical/Pharmaceutical Research
Currently use
Intend to use
None
Currently use
Intend to use
0
10
20
30
40
50
60
70
80
0
20
40
60
80
100

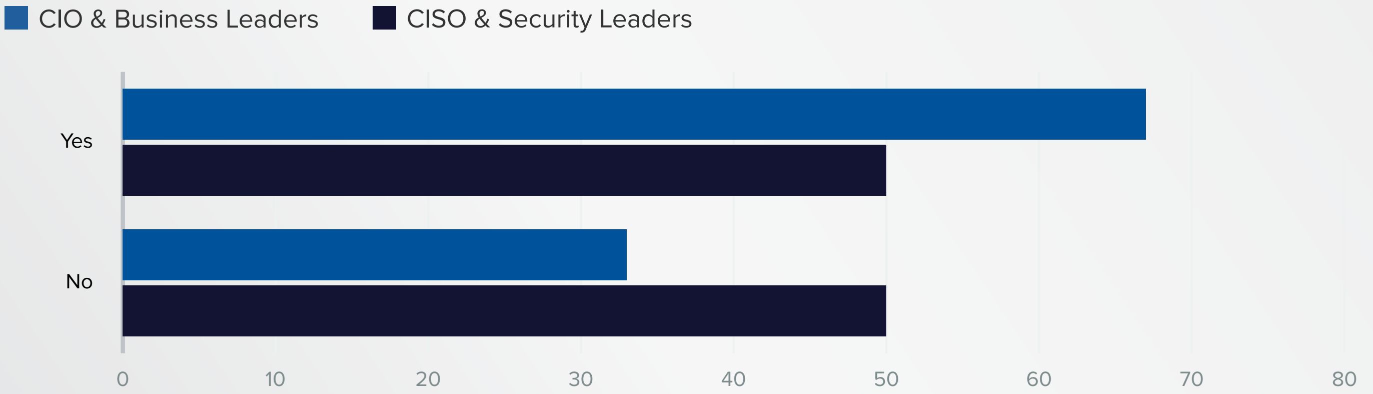
10. Do you have a specific budget for generative AI solutions?



Twenty-nine percent of business leaders report having a budget for generative AI solutions. None of the cybersecurity leaders say they do, although 14% say they don't know if they do.

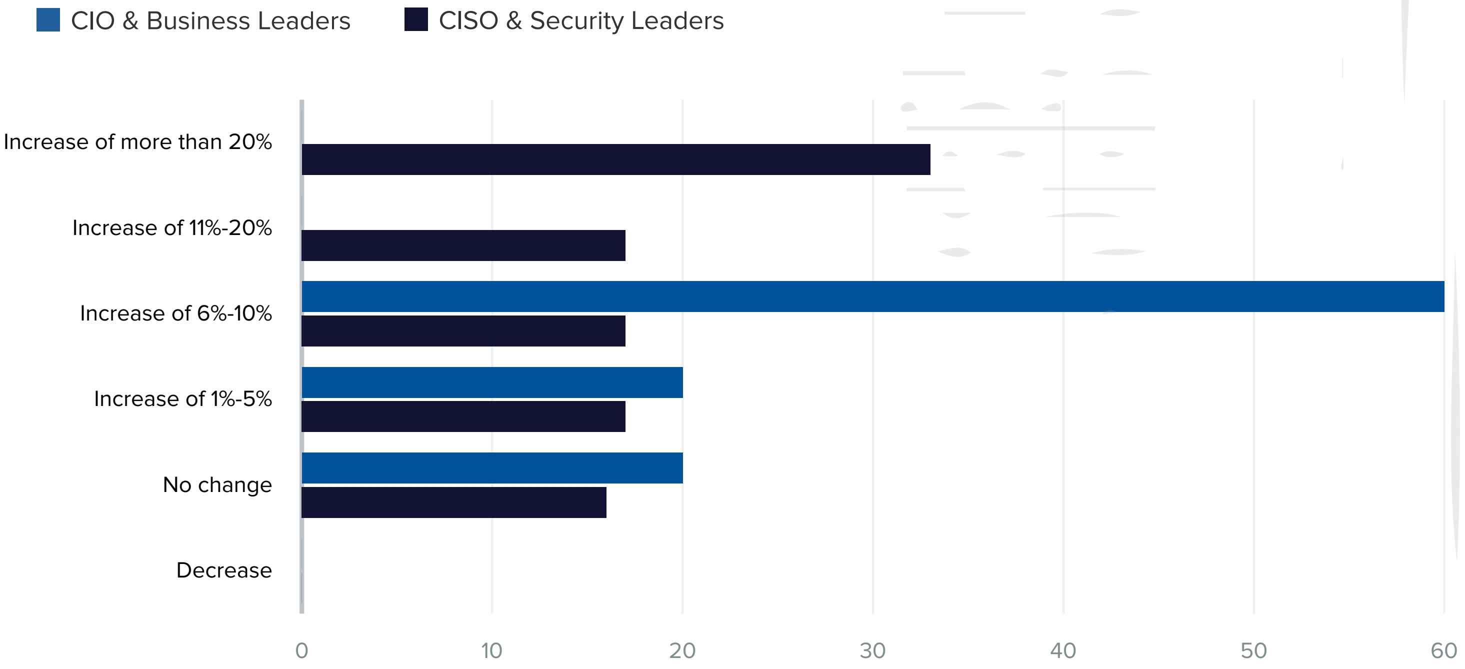
In the wider cohort, fewer business leaders and more cybersecurity professionals say they have a specific generative AI budget. Again, this is likely to reflect the health sector being behind in implementation.

11. If "no," do you expect to have one within 12 months?



Two-thirds of business leaders without a budget expect to get one within a year, and so do 50% of cybersecurity leaders. These figures are in line with other sectors.

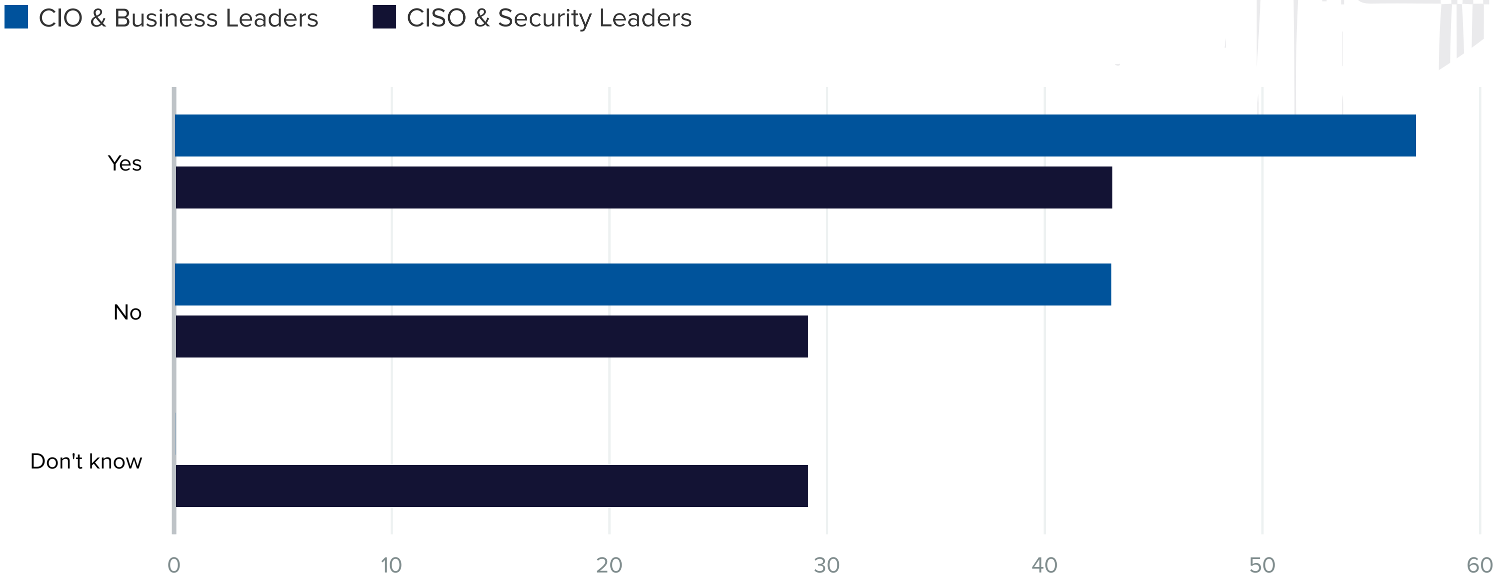
12. If "yes," what % increase in budget for generative AI solutions do you expect in 12 months' time?



Twenty percent of business leaders and 17% of cybersecurity leaders say they expect no change. Thirty-three percent of cybersecurity leaders expect an increase of more than 20%, while 60% of business leaders expect an increase of between 6% and 10%.

Compared to the wider cohort, fewer healthcare cybersecurity professionals expect no change in their budgets. But they are coming from a place of lower or nonexistent budget, so that is to be expected.

13. Do you have specific plans to purchase AI-driven solutions over the next 12 months for any of the use case options earlier mentioned?



Fifty-seven percent of business leaders have specific plans to purchase AI-driven solutions over the next 12 months, as do 43% of cybersecurity leaders.

These numbers are higher than for other vertical sectors, which is a surprise. But again, may reflect the healthcare sector coming from behind.

14. If "yes," please list up to top 5 desired use cases generative AI will address.

Among the use cases business leaders cite are BdM,Ex,BusEx and Scribe for patient reports, annotations, assistance in diagnosis, treatment, research - statistics, anomalous behaviors detection, initial containment/remediation for threats, and autonomous request resolution.

The use cases for the cybersecurity professionals are diagnosis and treatment of medical conditions, speed for code writing, newsletters and blog publishing, chatbots for customer support, code reviews, code generation, policy and standards, risk assessments, and vulnerability testing.

Understandably, this sector cites diagnosis and treatment of medical conditions.

15. What are your main concerns when it comes to implementing generative AI by yourself and/or by others?

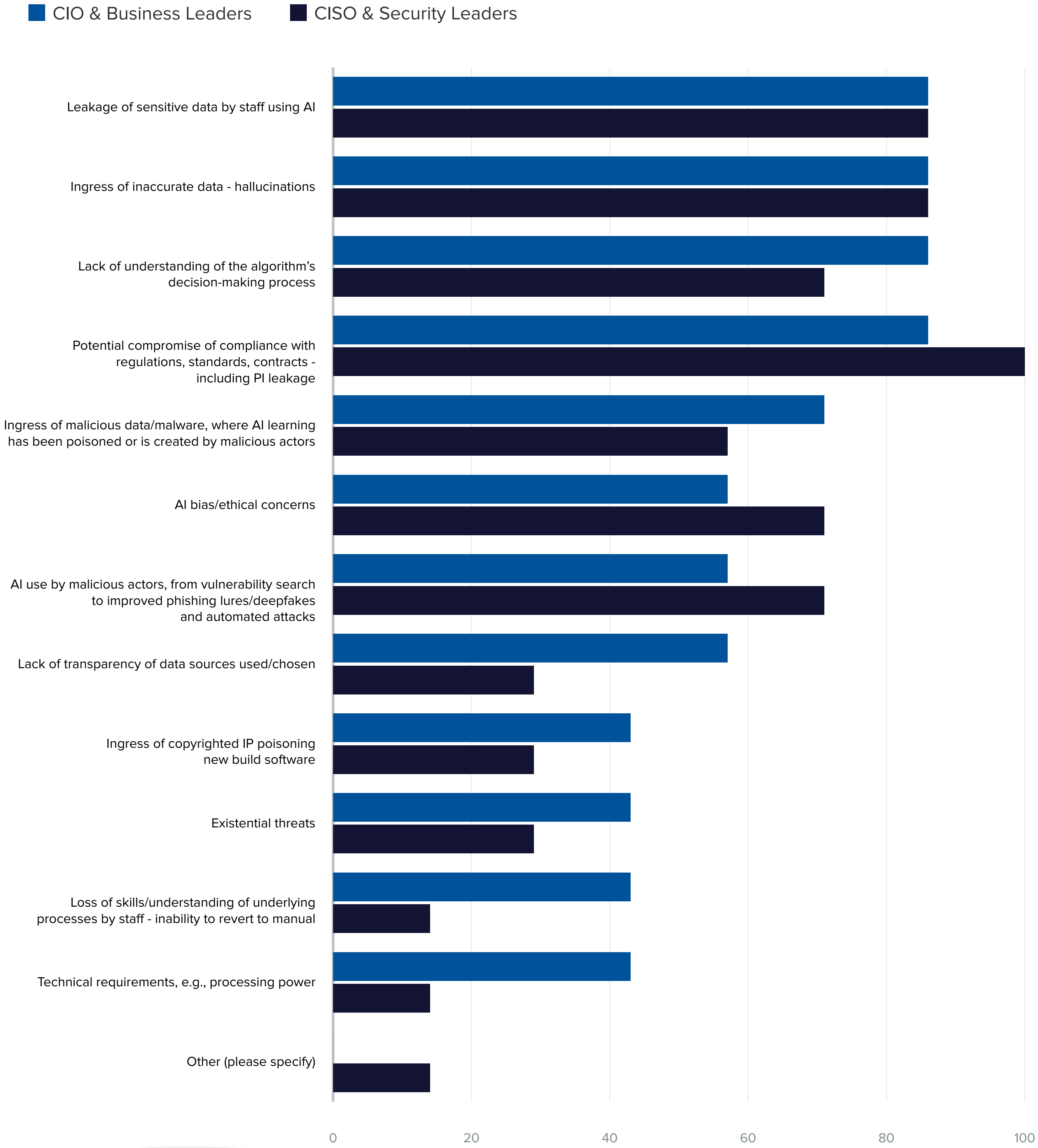
The top concerns of business leaders, each at 86%, are leakage of sensitive data by staff using AI, ingress of inaccurate data - hallucinations, lack of understanding of the algorithm's decision-making process, and potential compromise of compliance with regulations, standards, contracts - including PI leakage.

The top concern for cybersecurity professionals is potential compromise of compliance with regulations, standards, contracts - including PI leakage, at 100%. Leakage of sensitive data by staff using AI and ingress of inaccurate data - hallucinations are next, tied at 86%.

The top concerns are similar to those listed in other sectors.

FULL CHART ON NEXT PAGE

CHART 15


CIO & Business Leaders
CISO & Security Leaders
Leakage of sensitive data by staff using AI
Ingress of inaccurate data - hallucinations
Lack of understanding of the algorithm's decision-making process
Potential compromise of compliance with regulations, standards, contracts - including PI leakage
Ingress of malicious data/malware, where AI learning has been poisoned or is created by malicious actors
AI bias/ethical concerns
AI use by malicious actors, from vulnerability search to improved phishing lures/deepfakes and automated attacks
Lack of transparency of data sources used/chosen
Ingress of copyrighted IP poisoning new build software
Existential threats
Loss of skills/understanding of underlying processes by staff - inability to revert to manual
Technical requirements, e.g., processing power
Other (please specify)
0
20
40
60
80
100

16. What do you view as the biggest risk within code repositories in cybersecurity when it comes to generative AI use?

Business leaders cite unintended consequences and privacy concerns, lack of visibility, and security in general.

Cybersecurity professionals cite use by threat actors, consistency of decision-making, code errors, leakage of IP and insecure code.

17. What tools, processes or approaches do you currently use and intend to use to mitigate the concerns around use of AI by your own organization or your supply chain or partners?

Encryption of data: Eighty-three percent of board members and 80% of cybersecurity staff use it, and the remainder intend to use it.

Psuedoanonymization of data: One hundred percent of business leaders use psuedoanonymization of data, and 75% of cybersecurity leaders use it.

Walled garden - own AI: Twenty-five percent of respondents in each group use a walled garden, and the remainder intend to use it. The number intending to use a walled garden is higher than in other sectors.

Blocking software to prevent export of specified data types: Sixty-seven percent of business leaders use this, and 50% of cybersecurity professionals do. The remainder intend to use it.

Blocking software to prevent ingress of specified data/software categories: One hundred percent of business leaders use this, and so do 50% of cybersecurity professionals.

Whitelisting of specified generative AI: None of the business leaders use this, but 100% intend to use it. For cybersecurity leaders, 33% use it and the remainder intend to use it.

Blacklisting of specified generative AI: Fifty percent of business leaders use this; the rest intend to use it. For cybersecurity leaders, 33% use it and the remainder intend to use it.

Banning use of all generative AI: One hundred percent of business leaders use this, compared to just 25% of cybersecurity professionals. The remainder intend to use it. The numbers intending to ban use of AI are higher than in other sectors

Staff education and training around secure use of AI: Twenty percent of business leaders use this, and 33% of cybersecurity leaders use it. The remainder intend to do so.

AI-driven automated software from third party: One hundred percent of business leaders use this, and so do 33% of cybersecurity professionals. The rest intend to use it.

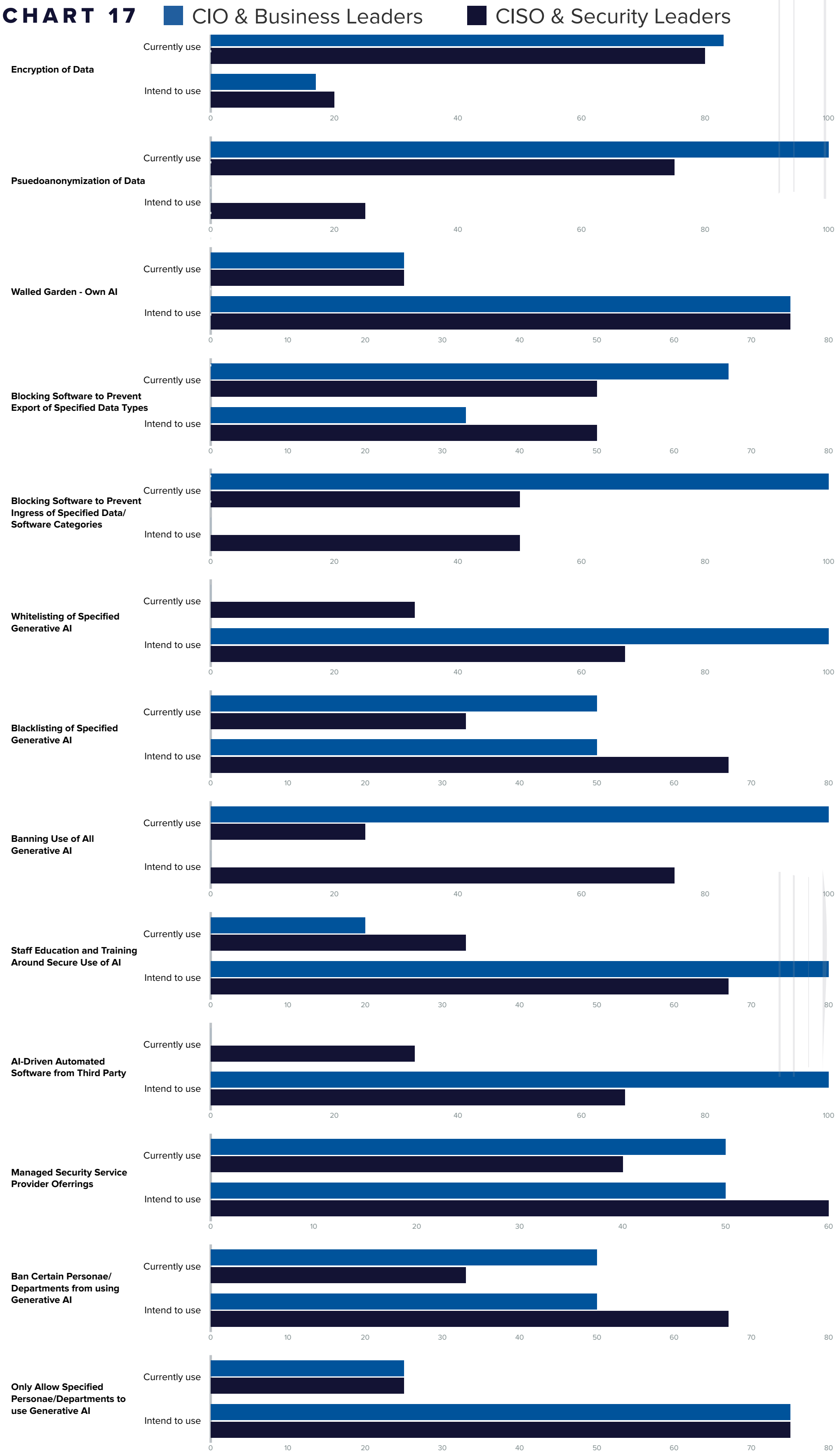
Managed Security Service Provider offerings: Fifty percent of business leaders and 40% of cybersecurity professionals use these, and the remainder intend to use them.

Ban certain personae/departments from using generative AI: Fifty percent of business leaders use this, as do 33% of cybersecurity professionals. The remainder in each group plan to use it.

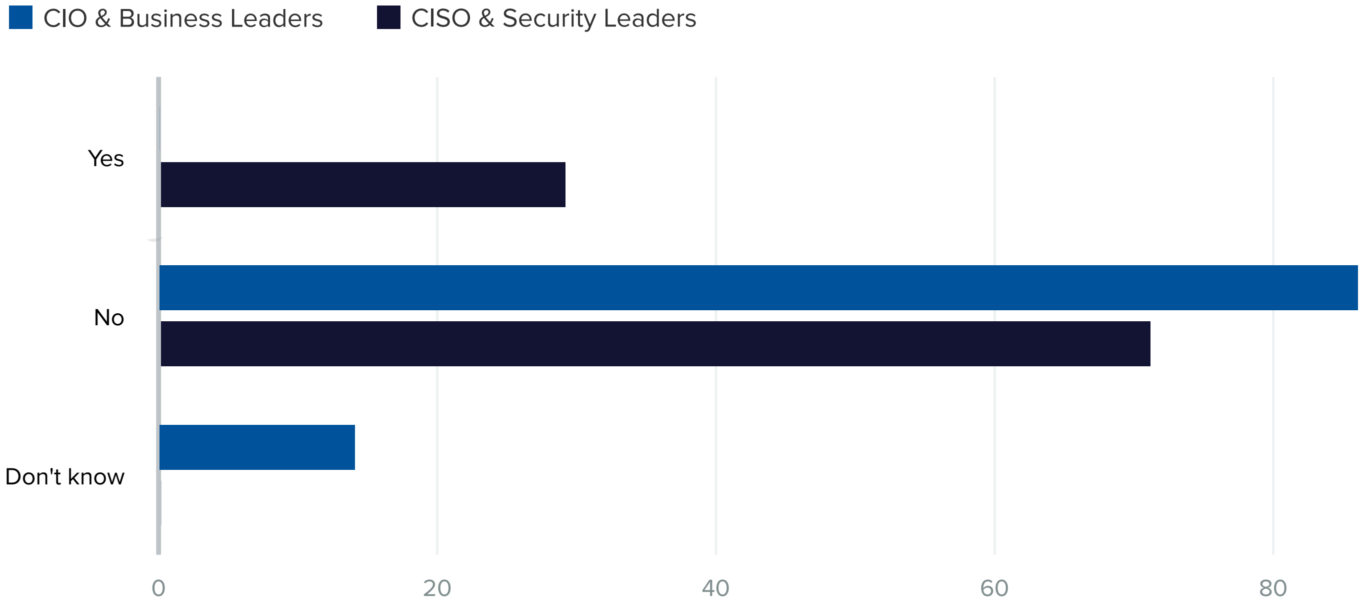
Only allow specified personae/departments to use generative AI: The figures for business leaders and cybersecurity professionals are the same: 25% use it and 75% intend to use it.

FULL CHART ON NEXT PAGE

CHART 17

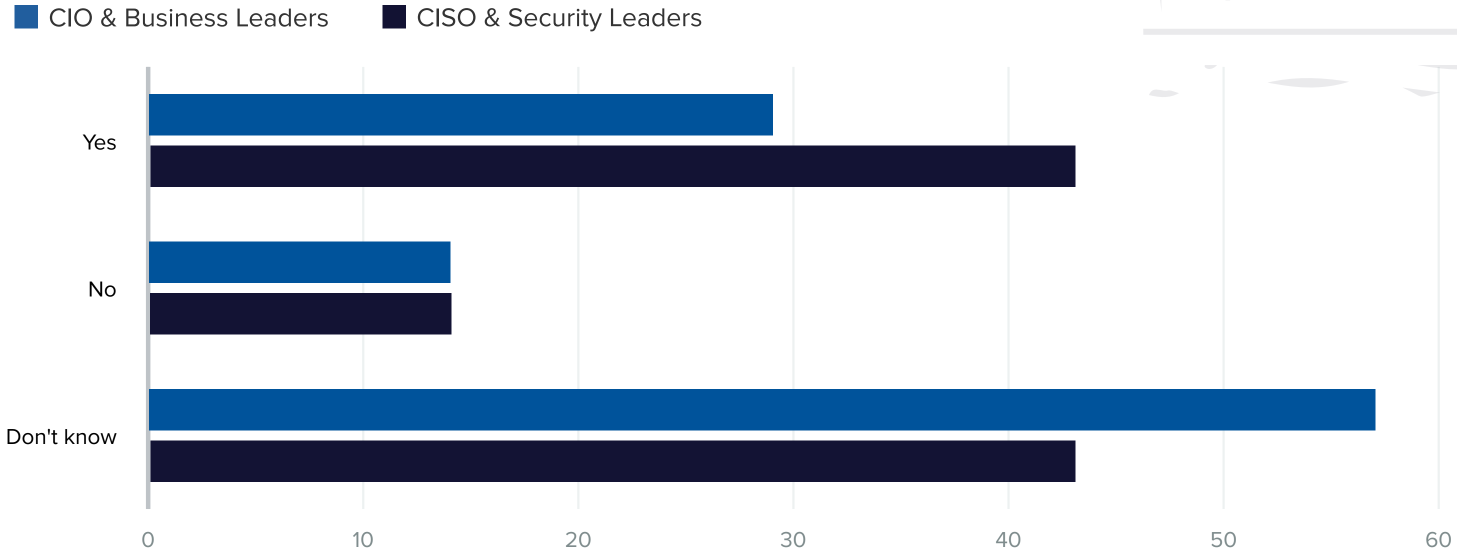

🟦 CIO & Business Leaders
■ CISO & Security Leaders
Encryption of Data
Currently use
Intend to use
0 20 40 60 80 100
Psuedoanonymization of Data
Currently use
Intend to use
0 20 40 60 80 100
Walled Garden - Own AI
Currently use
Intend to use
0 10 20 30 40 50 60 70 80
Blocking Software to Prevent Export of Specified Data Types
Currently use
Intend to use
0 10 20 30 40 50 60 70 80
Blocking Software to Prevent Ingress of Specified Data/ Software Categories
Currently use
Intend to use
0 20 40 60 80 100
Whitelisting of Specified Generative AI
Currently use
Intend to use
0 20 40 60 80 100
Blacklisting of Specified Generative AI
Currently use
Intend to use
0 10 20 30 40 50 60 70 80
Banning Use of All Generative AI
Currently use
Intend to use
0 20 40 60 80 100
Staff Education and Training Around Secure Use of AI
Currently use
Intend to use
0 10 20 30 40 50 60 70 80
AI-Driven Automated Software from Third Party
Currently use
Intend to use
0 20 40 60 80 100
Managed Security Service Provider Oferrings
Currently use
Intend to use
0 10 20 30 40 50 60
Ban Certain Personae/ Departments from using Generative AI
Currently use
Intend to use
0 10 20 30 40 50 60 70 80
Only Allow Specified Personae/Departments to use Generative AI
Currently use
Intend to use
0 10 20 30 40 50 60 70 80

18. Is there a process/playbook/guidelines/policy in place to ensure that all generative AI usage/deployment in your organization complies with agreed security policies?



None of the business leaders are aware of a process, playbook, guidelines or policy for their organization, and 29% of cybersecurity professionals are. The latter figure is in line with cybersecurity professionals in other sectors, but the figure for business leaders – zero – is much worse than the 30% for other sectors.

19. Do your competitors currently use generative AI?



Just 29% of business leaders and 43% of cybersecurity professionals say their competitors currently use generative AI. In both groups 14% say their competitors do not use it. The numbers for those who don't know are high in both groups, at 57% for business leaders and 43% for cybersecurity professionals.

20. Do you know and understand what regulatory restrictions/guidance applies to your use of generative AI in your geography/ industry vertical?

None of the business leaders know and understand what restrictions and guidance apply to their use of generative AI in their geography/ industry vertical, and 43% of cybersecurity leaders do understand. The zero for business leaders, compared to 60% in other sectors, shows that the healthcare business leaders appear to be lagging behind.

CONCLUSIONS

The healthcare sector is cautious about using AI but optimistic about potential gains.

The results from a small sample of the wider group suggest the medical sector's implementation of AI is more cautious than other vertical sectors and is behind in both implementation and pilots, which is not surprising given the higher risks involved with healthcare and greater regulation of the sector.

While both business leaders and cybersecurity professionals in healthcare are more cautious than other sectors, where permissions allow, there is a greater propensity within healthcare for cybersecurity leaders to adopt AI rather than business leaders. This suggests that where pilots do exist, they are likely to be practitioner-led rather than management-led.

That said, the business leaders are more optimistic about the level of gains than can potentially be achieved, more likely to plan specific purchases and expect budgets going forward. Both groups in the healthcare sector were more likely to ban the use of generative AI as a risk mitigation strategy than the wider cohort.

Cybersecurity leaders are ahead of business leaders in understanding AI.

Cybersecurity professionals were more likely to say they have and understand their playbook and understand the regulations that apply than their business leader compatriots. They are also more likely to believe they have responsibility for securing AI is within their remit, whereas the business professionals rarely assigned responsibility to CISOs.

Although similar trends were seen in the wider cohort, the extent of the divide suggests that there is a wider disconnect between business leaders and cybersecurity professionals within the health sector compared to other sectors.

Applying AI to Medical Results Analysis

TONY MORBIN: Medical results analysis was identified as one of the leading intended applications of generative AI by both business leaders and cybersecurity professionals. As somebody who does work with many leading health systems, what is your perspective of AI's applicability in this area?

DAVID BAILEY: As you look out across the healthcare ecosystem, there has been a trend over the last several years in how they can utilize technology and data analytics and advance the quality of care. When you add AI to that, you have things like the ability for machine learning algorithms to use neural networks that can register brain scans and 3D images thousands of times faster than other novel learning techniques. MIT researchers did this and described it. When you look at neural networks and how you can apply that in AI, you can take large amounts of data and predict output much quicker than you could before. If you look at the applicability from a quality of care perspective as well as the ability to identify a cancer cell much quicker than any normal scan today, the possibilities are endless on the valuecapability that AI-enhanced medicine can provide to us.

In Healthcare, AI Is Here

MORBIN: Obviously, AI has both pluses and minuses, so how would you describe the overall feeling about the introduction of AI within the healthcare ecosystem?

BAILEY: In a recent survey specific in healthcare, 500 providers were queried and I think 98% said that they were either planning to implement AI, had AI on the road map or were ready to embrace and use AI in their environment. I get the opportunity to speak to a lot of cybersecurity professionals inside of the healthcare ecosystem as well as leadership, and there has very rarely been a conversation over the last six months where AI hasn't been at least part of it. The awareness is starting to get there, and everyone has to be ready and prepared right now.

David Bailey
Vice President of Consulting Services
Clearwater

Dave Bailey is Vice President of Consulting Services at Clearwater and leads the managed and consulting services for the cybersecurity business. Before his role at Clearwater, he served as the Director of Technology and Security at Mary Washington Healthcare and was responsible for technology leadership, while serving as the HIPAA Security Officer.

Bailey received an Executive Master of Business Administration (EMBA) from Quantic School of Business and Technology and a BS in Computer Science from Wilkes University. He is a Certified Information Systems Security Professional (CISSP) and has spent the last 15 years in healthcare cybersecurity. He also has more than 12 years of cybersecurity experience serving in the Air Force and supporting the federal government in small and large businesses as a cybersecurity leader."

Security and Privacy Concerns

MORBIN: From your perspective, what are the most common security and privacy concerns about using AI in healthcare?

BAILEY: Let's look where the world is today from a healthcare perspective. The regulators and the Office forof Civil Rights have punitive actions for healthcare organizationscompanies that didn't do a proper risk analysis or didn't identify or manage risk. That is one of the biggest reasons why the OCR levies fines within the healthcare industry. Let's translate that to any use of technology. The first thing that has to happen is: Did you assess risk? Do you have a true understanding of what AI risks are? Do you have a good understanding of the potential impacts to the patient and to the data? How can you demonstrate that you've implemented reasonable and appropriate controls to protect the data?

With a traditional dataset, you give it some input and you get some output, and you know the output because it's from the dataset. But with AI, you have continual change of the dataset. If you have regulated data, data that's considered sensitive or data that needs to be protected, it is extremely important to have controls around that. Organizations need to understand what the risks are to that data, and not all organizations do a good job of that today. They're going to have to include that process with artificial intelligence as well.

The Biggest Risks

MORBIN: When organizations assess the security risks associated with AI, is it primarily about data, patient outcomes or regulatory compliance? What are the biggest risks?

BAILEY: It's a combination of everything that you just said. First and foremost, on the provider side, the number one risk is patient safety. Anytime AI is going to be used in a clinical care setting, you have to consider the safety of the patient. Look at the technologies that would impact direct clinical care and understand what the outcomes are. Understand the risks of using that technology. Then, go to the data. It's also extremely important to ensure that you're safeguarding the patient's data or any other data that's considered sensitive or classified. Threat actors are trying to get your data so you have to do what's reasonable and appropriate to ensure that you can protect whatever technology is using someone's data and provide reasonable and appropriate control around the data.

Ensuring Security With AI Use

MORBIN: What are your top suggestions for a healthcare organization that is looking to implement a tool using AI but wants to make sure they're maintaining a strong security posture?

BAILEY: Everything should start at the top. Ensure that you have governance around the use of AI and the use of all your data. The next step is to ensure that you have a good risk management framework. It's extremely important today to manage by identifying your risks, understanding what those risks are, and putting in the appropriate measures in order to respond to those risks.

There are a lot of great practices that people can implement within governance and risk management, but there are some new things that every organization will have to consider if they're starting to implement and use their own AI technologies. One is trustworthiness, which NIST described in their risk management framework. How can you determine that the system that you're using is trustworthy? What are the mechanisms? Are there mechanisms to ensure that the outcomes you get are trustworthy?

Some practices are going to be new to everyone, and we need to understand how AI may change the existing way that we think about the life cycle of data and data governance. We all need to be educated in what those things are and recognize that we may have to change our way of doing the practices that we're doing today. It's still going to all be around the data and how your organization can determine the trustworthiness of AI as they implement it within their environment.

> We need to understand how AI may change the existing way that we think about the life cycle of data and data governance.
>
> - David Bailey

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io • research@ismg-corporate.io

BANK INFO SECURITY® CAREERS INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

CU INFO SECURITY® Just for Credit Unions · Data Breach TODAY® Prevention. Response. Notification. · infoRisk TODAY® · AIToday.io · CIO.inc

CyberEd.io · CyberEdBoard · DeviceSecurity.io · FraudToday.io · PaymentSecurity.io

CYBER THEORY · GREYHEAD AN ISMG COMPANY · Xtra mile LIFECYCLE MARKETING

iSMG

902 Carnegie Center • Princeton, NJ • 08540 • ismg.io