sas | intel | Microsoft | ISMG

Fighting Fraud and Financial Crime

Assessing the Impact of AI and Other Change Agents

INTRODUCTION

The continuing battle against fraud and financial crime demands constant adaptation and innovation. Generative AI (Artificial Intelligence) and broader AI technologies have brought both excitement and apprehension to our field, as they hold the promise of revolutionising our approach to fraud prevention while introducing new challenges. Better understanding of the opportunities and challenges can help us assess potential use through a measured lens.

Our survey presented a unique opportunity for Fraud, AML, Financial Crime (FC) and Compliance professionals to share insights and contribute to a deeper understanding of how AI and other transformative technologies are influencing our daily fight against fraud.

Among the research focused survey questions to be answered:

- How is AI currently being harnessed in the banking sector to combat fraud and financial crime?
- What benefits and risks are associated with the expanding integration of AI in fraud/financial crime detection and prevention?
- What are the regulatory and compliance implications of implementing AI solutions in fraud and financial crime prevention?

Enjoy the insights and the analysis of what these survey results mean and how they can be put to use.

Best,

Tom Field
Senior Vice President, Editorial
Information Security Media Group
tfield@ismg.io

TABLE OF CONTENTS

About this survey:

This survey was conducted in late Q4, 2023. It focused on banking across the ASEAN, India, Hong Kong and Australia and New Zealand (ANZ) regions. The survey attracted more than 100 responses from Fraud, AML, and Compliance professionals. Of the respondents, 47% are from organisations of up to 5,000 employees; 24% are from organisations between 5,000-20,000 employees; 11% represent entities of 20,000-50,000 employees; and 18% are from organisations of over 50,000 employees.

About SAS

SAS is the global leader in analytics. We inspire our customers to transform data into intelligence. And in a digital world where fighting fraud and financial crime grows more complex by the day, SAS delivers the most innovative advanced analytics and AI technologies to keep you ahead.

With a 49-year heritage and deep industry expertise, SAS is a trusted partner to organisations seeking immediate value from their data. We help businesses solve their toughest challenges with greater speed, scale and efficiency.

SAS integrated solutions include a risk-based approach to monitoring for laundering and terrorist financing activities; the ability to rate new and existing customer scores based on key events and new information; identify and prevent first-party application and payments fraud; detect, prevent and manage fraud enterprise-wide in real-time; and address a wide variety of intelligence analysis and investigation management needs quickly and precisely.

About Intel

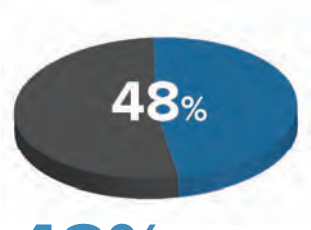
Intel (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better. To learn more about Intel's innovations, go to newsroom.intel.com and intel.com.

About Microsoft

At Microsoft, our mission is to "empower every person and every organization on the planet to achieve more". Over the last three decades, we've helped people and organisations use technology to transform how they work, live and play. Over the next decade, we have a generational opportunity to come together to build a better future marked by sustainable economic growth and opportunity for all. Azure's innovation platform enables unique customer experiences and app growth through migration, modernization, and intelligence.

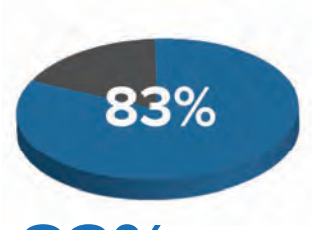
BY THE NUMBERS

Statistics that jump out from this study:



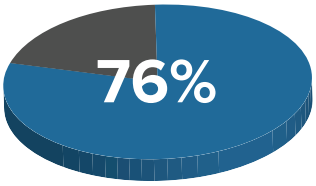
48%

of respondents say they currently use AI/ML/analytic-based detection.



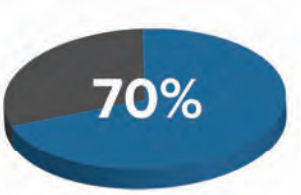
83%

say they will invest in other AI techniques in 2024.



76%

say key AI benefits include improving operational efficiency and effectiveness.



70%

say their biggest concern about AI in the hands of adversaries is deepfakes created by attackers.

EXECUTIVE SUMMARY

"We're still developing our internal policies."

"We're creating use cases and POCs."

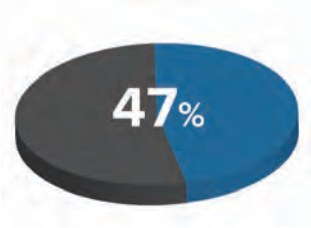
"We need to build guardrails around it."

These are some of the most common enterprise reactions to the explosion of generative AI, which blossomed globally in 2023 in a way unmatched by any previous emerging technology.

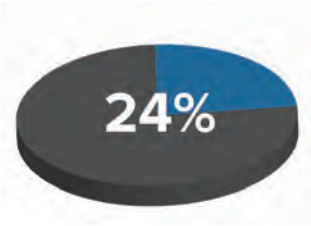
Yet, while many organisations worldwide are taking a cautious approach to developing their own use cases, Asian banking institutions articulate real progress in embracing generative AI to help battle fraud and financial crime.

ABOUT THESE RESPONDENTS:

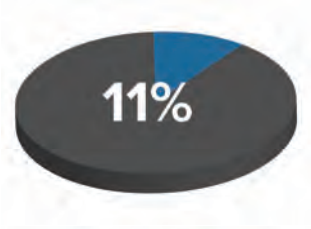
These are not small organisations toying with generative AI. Of the 100 respondents to this survey:



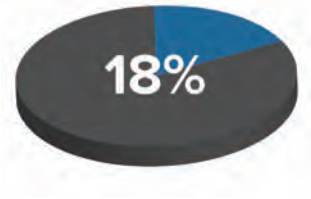
47%
are from organisations of up to 5,000 employees;



24%
are from organisations between 5,000-20,000 employees;



11%
percent represent entities of 20,000-50,000 employees;



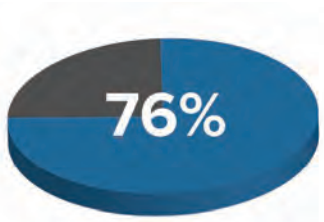
18%
are from organisations of over 50,000 employees.

When considering the core capabilities of AI, such as Machine Learning and advanced analytics in this survey of banking institutions in the ASEAN, India, Hong Kong and ANZ regions:

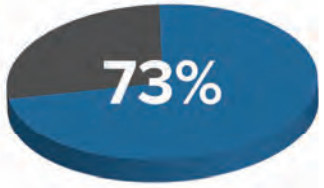
Nearly 50% of respondents say they currently use AI/ML/ analytic-based detection.

20% say they use other AI techniques, and 83% say they plan to use them in the next 18 months.

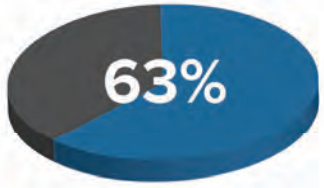
Asked what they see as the key potential benefits of applying AI against fraud and financial crime, respondents say:



Improving operational efficiency and effectiveness - **76%**



Better prioritising identified risks and reducing alert volumes - **73%**



Identifying additional risks - **63%**

KEY FINDINGS:

This survey set out to answer three key questions:

1 How is AI currently being harnessed in the banking sector to combat fraud and financial crime?

Forty-five percent of respondents say it "acts as an overlay in combination with other techniques to improve operational efficiency and effectiveness of current systems."

2 What benefits and risks are associated with the integration of AI in fraud detection and prevention? Respondents were asked to select their top three potential benefits:

- Improving operational efficiency and effectiveness, including better prioritising identified risks and reducing alert volumes - 73%
- Identifying additional risks - 63%
- Automating business or technology processes - 53%

a. When asked to name the top three challenges for their organisation to use AI, they say:

- Organisational readiness of resources needed to develop/apply AI - 52%
- Concern over the ethics of using AI - 49%
- Inability to verify accuracy of results/identify errors - 43%

b. Respondents' top fears about criminals employing AI in their schemes are:

- Deepfakes created by attackers - 70%
- More effective lures for phishing texts - 51%
- AI use for crime at scale - 51

3 What are the regulatory and compliance implications of implementing AI solutions in fraud prevention?

Nearly 70% of respondents say regulators are influencing the landscape by introducing new regulations to drive reduction in risk or loss.

Eighty-six percent say these activities are influencing their investment/resource allocation in some way – the top being increased operational resources responsible for work items identified by risk systems - 55%.

OTHER KEY FINDINGS

There are commonalities among these respondents:

- **69%** feel their fraud and financial crime exposure is the same or greater than their peers.
- **73%** feel their exposure is the same or more than last year.

Asked to list their top three crime exposure types of concern, respondents say:

- Third-party-actioned compromise - **71%**
- First-party-actioned scams - **51%**
- Collusive activities - **37%**

Asked to list the top three main compromise routes, they say:

- Email - **73%**
- SMS text/instant message - **49%**
- Social media - **45%**

The top three techniques organisations plan to use within 18 months to identify additional exposures/risks are:

- Other AI techniques - **83%**
- Graph DB - **73%**
- Financial intelligence units - **63%**

SOME OTHER NOTABLE FINDINGS:

Reference Data: Seventy-four percent of respondents use at least some form of reference data to tackle fraud/crime challenges. The top forms are credit bureau/reference data at 49% and device and/or session data at 43%.

Crypto and Blockchain: The top three concerns about the impact of crypto and blockchain are:

- Anonymity of ownership prevents KYC checks - 55%
- Anonymity of ownership facilitates money laundering - 46%
- Anonymity of ownership aids payments to extortionists, fraudsters and other criminals - 42%

Cloud: Only 5% of respondents have no plans to use cloud for solutions/data processing. Thirty-two percent say they already do it.

Data Residency: Twenty-seven percent still store critical data on-premises but are considering cloud options, and 43% say they have geographic regulatory requirements for data residency.

CONCLUSIONS

Read on for full survey results, expert analysis and conclusions. To summarise the conclusions:

- **It's Early Days - But Move Quickly:** To this point, only 48% of respondents say they are employing AI in their analytics-based detections. But 83% say they intend to deploy other AI in the year ahead. This "full speed ahead" strategy is sound, given the speed of AI including generative AI adoption and the real-world use cases that show efficiencies and insights to be gained from further enhancing and/or automating fraud/crime detection.

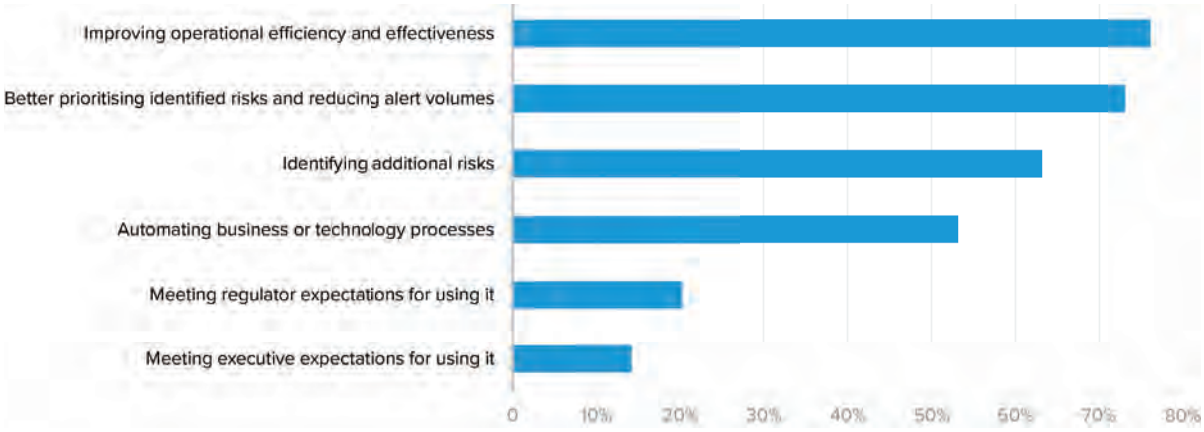
- **Build Those Use Cases:** Anomaly detection is the place to begin. Integrate data sources into an AI-driven engine that can find the anomalies and highlight the risks. Let the machine do the early detection. Where possible allow AI to take the initial burden away from manual resources and free their time to analyse and respond. Using them when alerts require intervention and investigation. And do not discount the value of a hybrid approach to adopting AI solutions. There is no need to abandon tools that work. AI intends to enhance them.

- **Keep Your Eyes on Adversaries and Regulators:** Criminals are using AI, too, but you will be seeing more targeted scam campaigns as fraudsters too benefit from efficiencies and automation. AI has not yet reached its peak as a key weapon for adversaries in committing fraud and financial crime. Similarly, as evidenced by the recent passage of Europe's AI Act, regulators are paying attention to the rise of AI including generative AI, and regulatory leadership may well emerge in the markets covered by this survey. Let’s hope regulation does not restrict its power and usage unfairly, but perhaps it will.

SURVEY RESULTS

Fraud and Financial Crime: The Impact of AI and Other Change Agents

1. What do you and/or your organisation view as the key potential benefits of applying AI in combating fraud and/or financial crime? Select your top 3.



The leading potential benefit of applying AI to combat fraud and/or financial crime identified by respondents is improving operational efficiency and effectiveness – cited by 76%. It seems that the primary benefit sought is not so much revolutionary change, but doing what they currently do, better. This is closely followed by the related issue of better prioritising identified risks and reducing alert volumes at 73% – again, addressing a current pain point of alert overload through more intelligent automated processes.

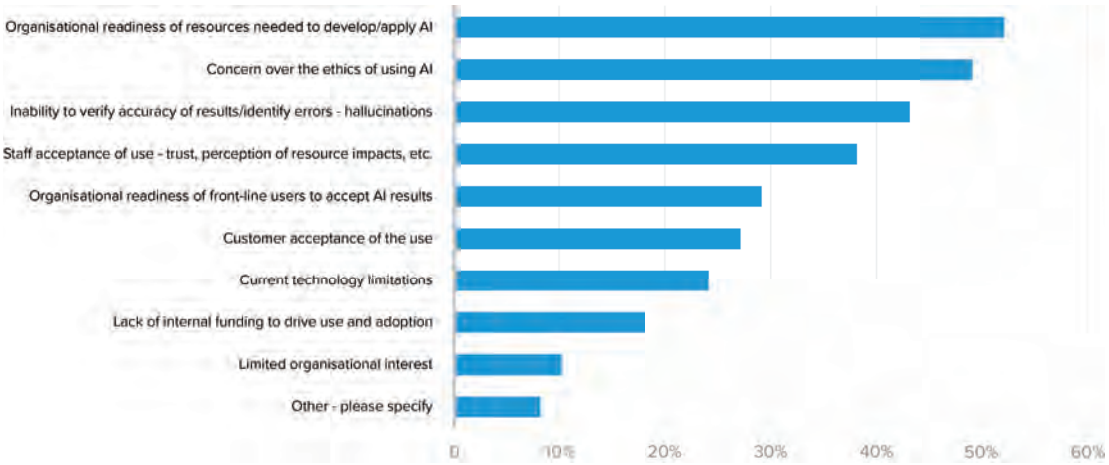
Third on the list is the first mention of using AI for innovative improvement, and that is the 63% of respondents who cite identifying additional risks. Just over half - 53% - mention automating business or technology processes – again, something that has been possible and implemented by many prior to the advent of widespread availability of generative AI.

Meeting executive and regulator expectations for use – at 14% and 20% respectively, is appropriately lower down the list, suggesting that real use cases, rather than a checkbox exercise, are driving uptake.

Nonetheless, these use cases are strongly led by increasing the efficiency of current approaches rather than innovative new approaches. The publicity around AI capabilities also appears to be stimulating the automation laggards to address this deficiency in their operations.

That said, the inclusion of identifying additional risks as third on the list suggests there is clearly also an awareness of the possibility of innovative implementations, and these are likely to increase as familiarity with capabilities grows.

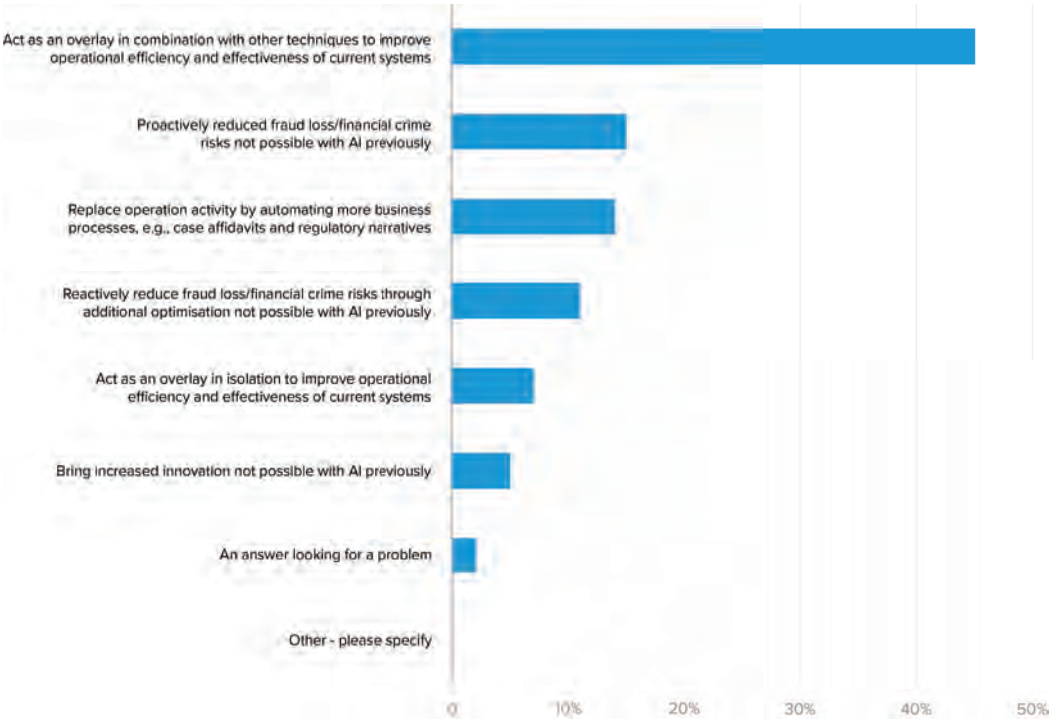
2. What do you feel may be the top challenges for your organisation to use AI? Select your top 3



Asked about their single top challenge to the implementation of AI, respondents offer two very different challenges, both cited by roughly 50%: Organisational readiness of resources needed to develop/apply AI is the top response at 52%, and concern over the ethics of using AI follows at 49% – thus one operational concern and one strategic.

Third on the list is inability to verify accuracy of results/identify errors, at 43% – thus again operational in terms of quality control/reliability. Only 10% cited limited organisational interest.

3. Considering the opportunity for use of generative AI, which areas do you assume or perceive will gain most when applied to combat fraud and financial crime?

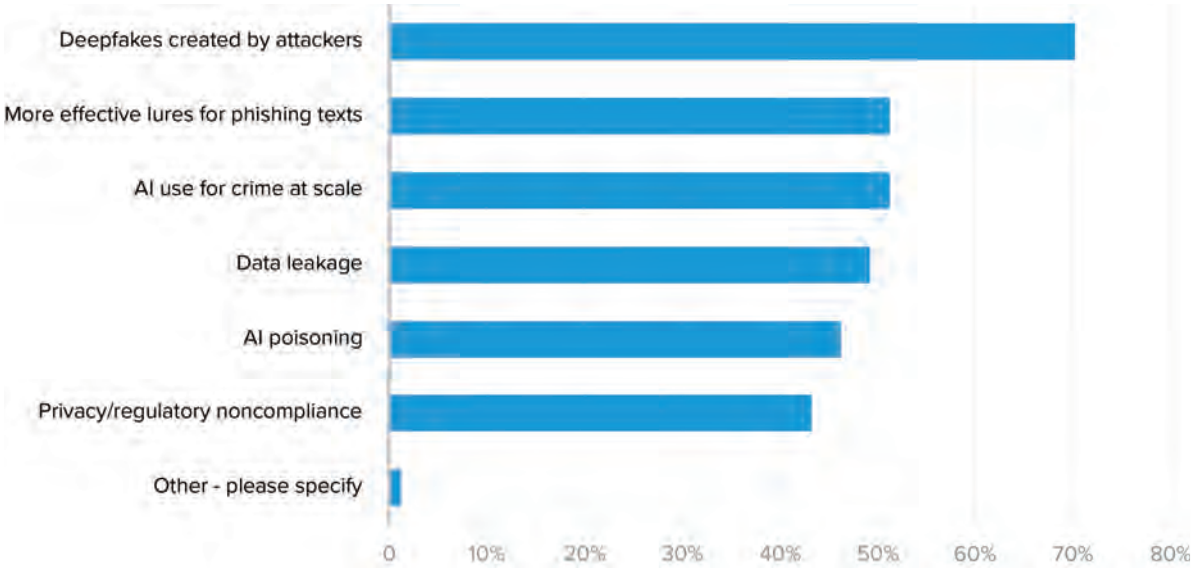


While there is a clear front-runner when it comes to leading assumptions or perceptions of which areas will gain most when applying generative AI to combat fraud and financial crime, none of the options gained overwhelming support. The lead use case for 45% of respondents is for AI to act as an overlay in combination with other techniques to improve operational efficiency and effectiveness of current systems. Again, this reflects the earlier approach of improving current activities.

Quite some way behind at 15% is to proactively reduce fraud loss/financial crime risks not possible with AI previously – which probably identifies the true proportion of those at the leading edge of AI implementation, along with the 5% who cited bringing increased innovation not possible with AI previously.

Just behind in third place at 14% is replacing operational activity by automating more business processes, e.g., case affidavits and regulatory narratives. Again, this is perhaps reported by the laggards in the automation stakes who are realising that the time/opportunity to automate is now.

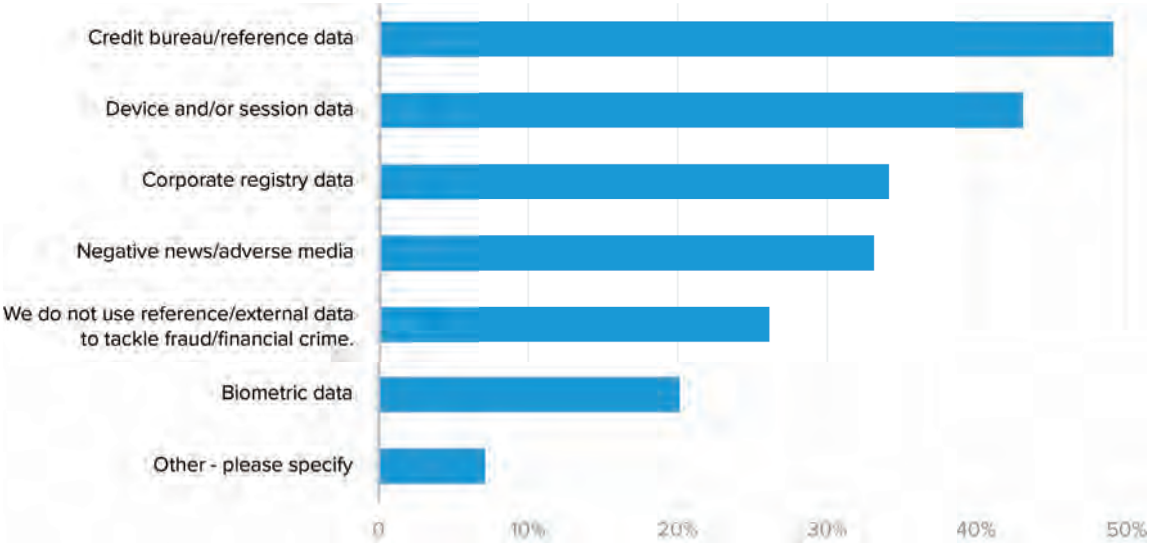
4. What are your primary concerns regarding criminal use of AI? Select your top 3.



Appropriately enough for a sector that has always faced criminal adversaries, there was more consensus when it came to concerns around the implementation of AI.

The leading concern, at 70%, is deepfakes created by attackers – no doubt reflecting that real world cases have already occurred. This is followed, perhaps surprisingly far behind given AI's capabilities, with AI use for crime at scale tied with more effective lures for phishing texts, both at 51%, followed by data leakage at 49%. In the same ballpark is AI poisoning, or tampering with an AI model's training data, at 46% and regulatory/privacy compliance at 43%.

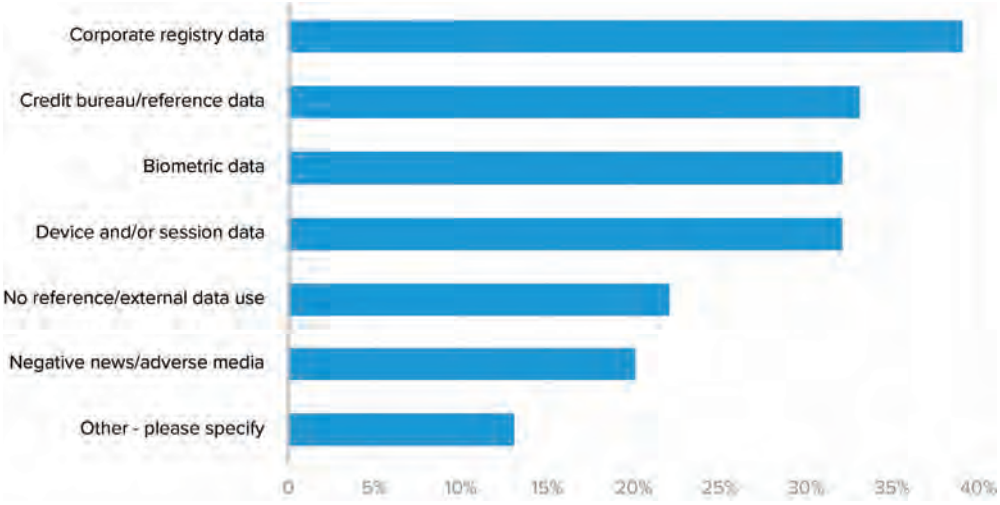
5. Does your company use reference data to tackle your main fraud or financial crime challenges and if so, what types of data do you use? Check all that apply.



Credit bureau/reference data is the top use of reference data to tackle main fraud or financial crime challenges, but even so it is used by less than half of respondents – 49%. This is followed by device and/or session data at 43% and corporate registry data at 34%.

Thirty-three percent cite negative news/adverse media as a main source of reference data, and just over one-quarter - 26% - say they do not use reference/external data to tackle fraud/financial crime. Only 20% of respondents report using biometric data.

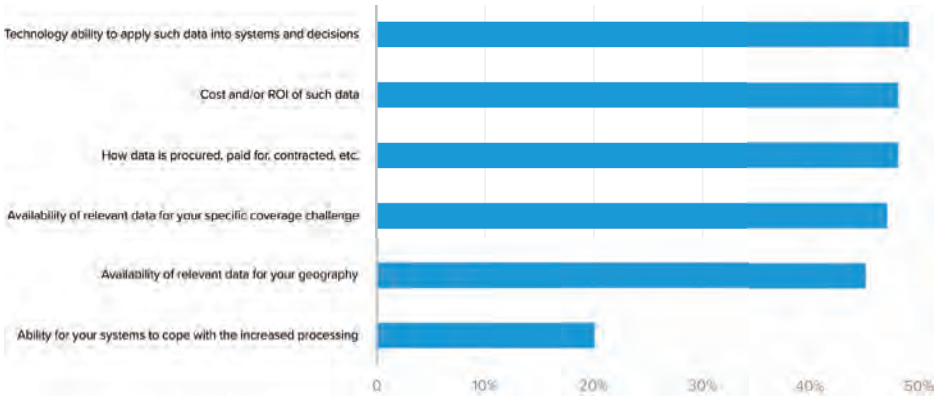
6. In the next 18 months, which reference data that you are not currently using do you expect to begin using to tackle your main fraud or financial crime challenges? Check all that apply.



The figure for those who do not expect to use reference/external data - 22% - is not far from the 26% who do not currently use it, suggesting that no rapid change is expected in the uptake of external reference data.

But among those who plan to start using additional reference data, the biggest anticipated increase in usage is in corporate registry data. Thirty-nine percent of those not currently using it say they expect to begin using it within 18 months. This is followed in second place by credit bureau/reference data at 33% and biometric data and device and/or session data, tied at 32%.

7. What are your biggest challenges in using external/reference data? Select your top 3.

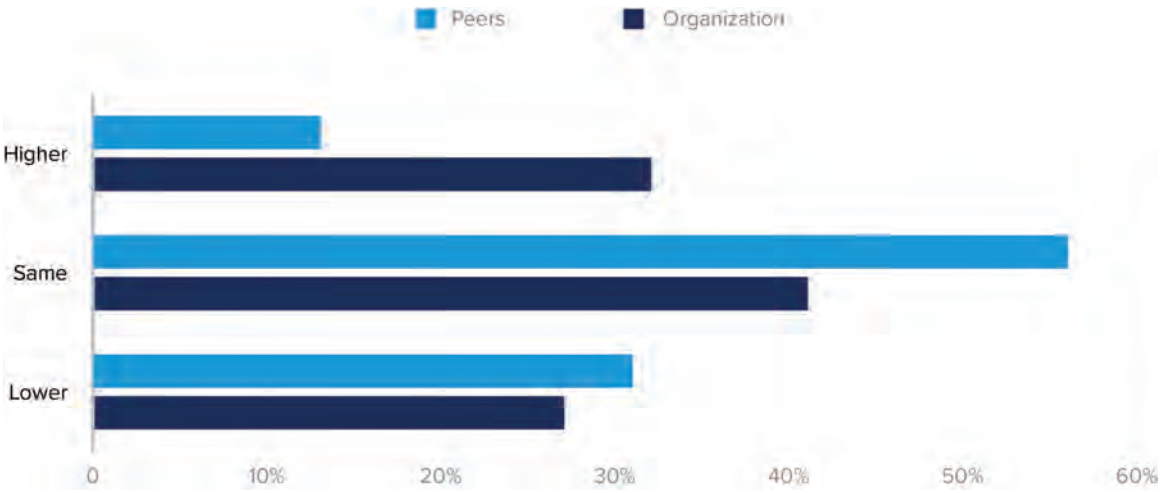


The biggest challenge in using external/reference data is technological ability to apply such data into systems and decisions, at 49%, but this just edged out two factors: cost and/or ROI of such data and how data is procured, paid for, contracted, etc. – both at 48%.

Just behind in third place is availability of relevant data for your specific coverage challenge at 47%, closely followed by availability of relevant data for your geography at 45%.

In summary, it would appear a near equal tie for the cost/reward equation and ability to make best use of reference data are the key challenges to increasing uptake. This suggests simplified ability to use and cost-justify data might ease the financial constraints.

8. How is your fraud and financial crime risk exposure compared to your peers/your organisation last year?



Asked to compare themselves to peer organisations, 87% of respondents believe that their fraud and financial crime risk exposure is the same as - 56% - or lower than - 31% - their peers. There are still 13% who recognise that their exposure is higher than that of their peers.

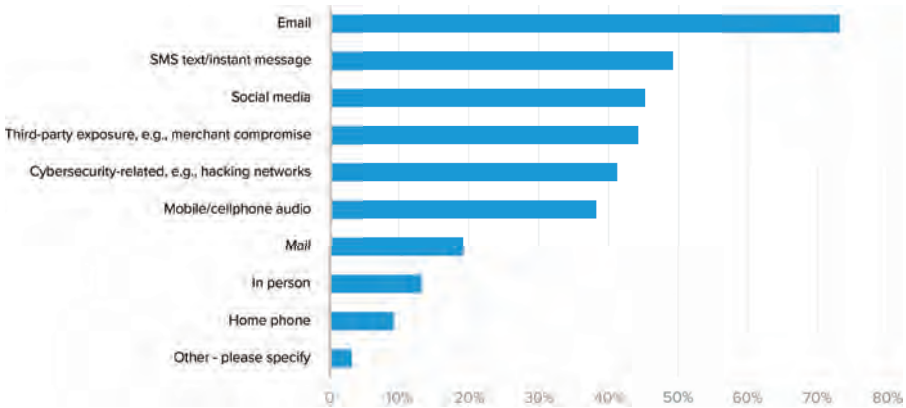
Furthermore, 32% believe their risk exposure is higher than the previous year, 41% say it is unchanged, and 27% feel their exposure is lower than it was a year ago.

9. What exposure types are most concerning for your organisation? Select your top 3.

The exposure type respondents say is most concerning for organisations is third-party-actioned compromise, e.g., resulting from phishing, at 71%. This is followed some way behind by first-party-actioned scams, e.g., Authorised Push Payment, at 51%. In third place is collusive activities, e.g., internal/employee and insider, at 37%, followed by monitoring of complex typologies - trafficking, trade-based, kleptocracy at 36%.

Yet again, the concerns – no doubt representing actual historic experience – reflect current main attack types and do not yet indicate the uptake of AI by criminals. Or it may be that most criminals use AI simply to make their current activities more efficient rather than to conduct new types of attacks.

10. What are the main routes you see attackers using to initiate compromise? Select your top 3.

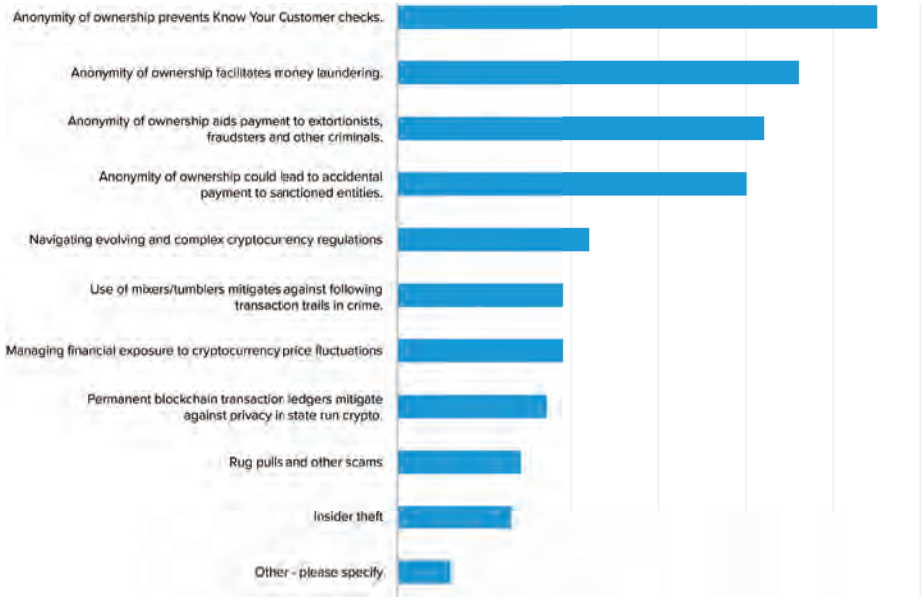


Reflecting the concern over phishing cited earlier, the main compromise route respondents see attackers using to initiate compromise is email, at 73%.

A few of the responses reflect the rise in mobile attacks – including the number two attack vector, SMS text/ instant message, at 49%, and number six, mobile/cellphone audio, at 38%. The home phone comes last at just 9%, behind mail at 19%.

Social media remains a concern at 45%, and so does third-party exposure, e.g., merchant compromise, at 44% and cybersecurity-related, e.g., hacking networks at 41%.

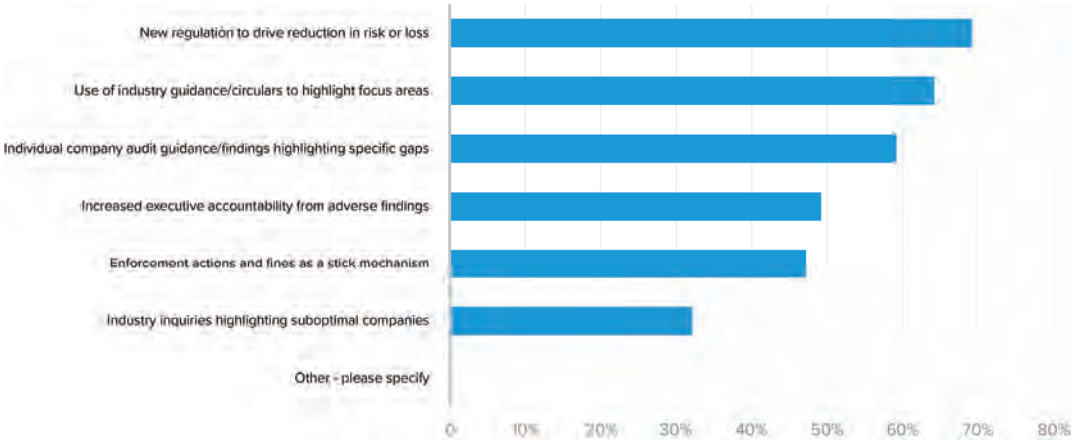
11. What are your primary concerns regarding the impact of crypto and blockchain on your organisation? Select your top 3.



Compliance appears to be the top concern around the impact of crypto and blockchain on organisations, as 55% cite anonymity of ownership preventing Know Your Customer checks. This is also reflected in the second-most-cited concern, anonymity of ownership facilitating money laundering, at 46%.

The third and fourth leading concerns again relate to the anonymity of ownership, with anonymity of ownership aiding payment to extortionists, fraudsters and other criminals at 42% and anonymity of ownership leading to accidental payment to sanctioned entities at 40% – again a compliance issue.

12. How are you seeing regulators affect the overall fraud and/or financial crime landscape in your geography? Check all that apply.

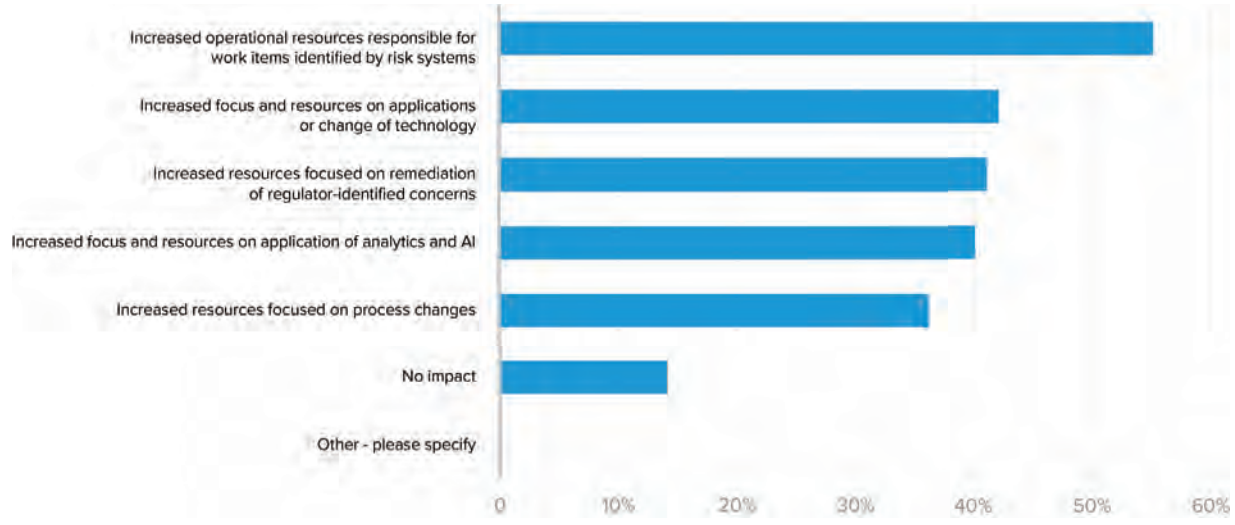


When specifically asked how they see regulators affecting the overall fraud and/or financial crime landscape in their sector, the respondents' leading, and very positive response, is expectation that new regulation will drive reduction in risk or loss, at 69%. This is followed by use of industry guidance/circulars to highlight focus areas at 64%, and individual company audit guidance/findings highlighting specific gaps at 59%.

Next come positives about which some respondents may be more ambivalent – increased executive accountability from adverse findings at 49%, enforcement actions and fines as a "stick" mechanism at 47%, and industry inquiries highlighting suboptimal companies at 32%.

The responses suggest both understanding and acceptance of the positive role regulations play in the APAC financial sector as a whole.

13. How are regulator activities driving your organisational investment and resource allocation in addressing fraud and/or financial crimes? Check all that apply.

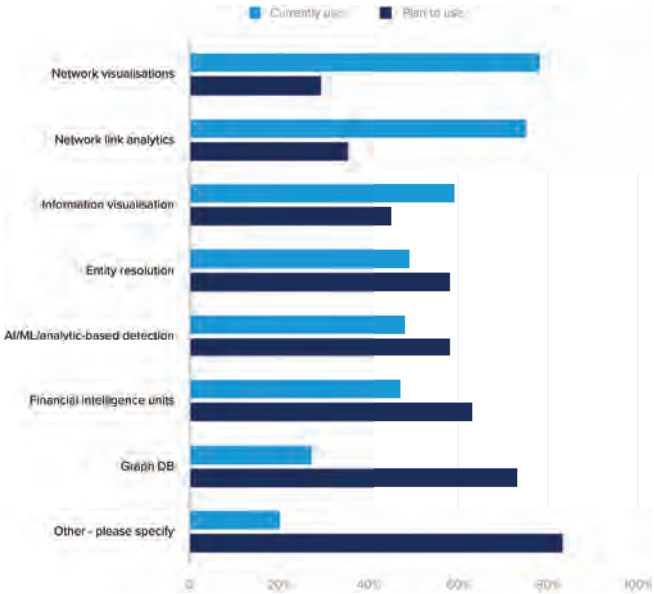


When asked how regulator activities are driving their organisational investment and resource allocation in addressing fraud and/or financial crimes, 55% of respondents say regulator activities have increased their number of operational resources responsible for work items identified by risk systems, followed by 42% who say the activities have increased their focus and resources on applications or change of technology.

Forty-one percent say regulator activities have increased their resources focused on remediation of regulator-identified concerns, and 36% say they have increased their resources focused on process changes.

Just 14% said regulator activities have had no impact.

14. What techniques is your organisation currently using or planning to use within 18 months to identify additional exposures/risks? Check all that apply.



The standout techniques respondents say their organisations currently use to identify additional exposures/risks are network visualisations at 78% and network link analytics at 75%. "Other" AI techniques beyond those listed comes in last at 20%.

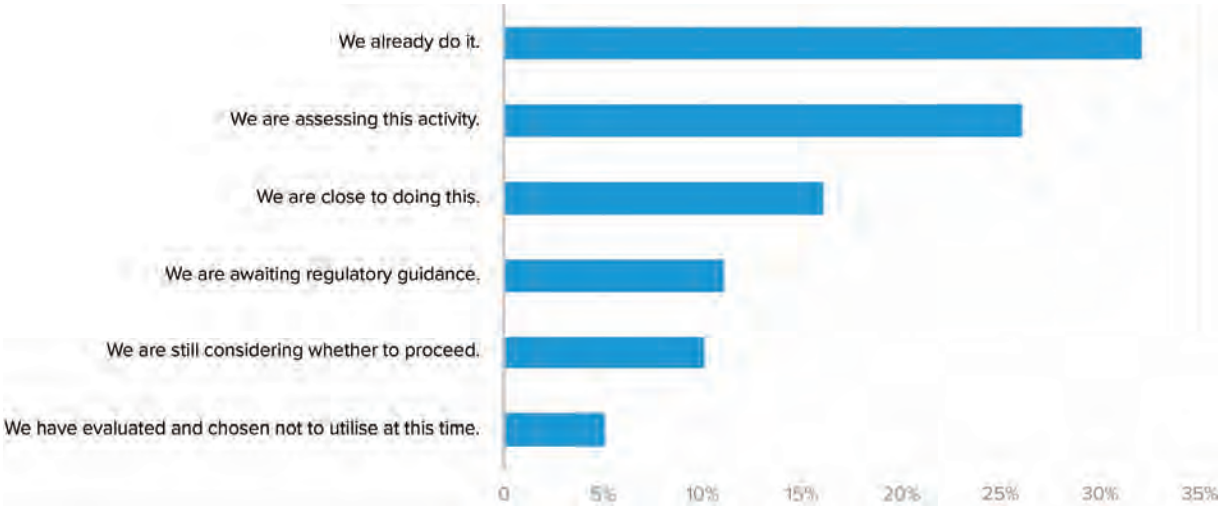
But when asked which techniques their organisations plan to use within 18 months, the last become first. "Other" AI techniques is at 83%, and new adoptions of network visualisations is at 29% and network link analytics is at 35%.

The other big riser is Graph DB, which respondents say is set to increase from 27% using it currently to 73% adopting it over the next 18 months.

While growth in uptake will be lower for already widely adopted approaches, the scale of growth in other AI techniques – at a projected 400% in 18 months – is both phenomenal and unsurprising.

Organisations clearly recognise that new game-changing options are arriving rapidly, and they anticipate adoption, notwithstanding concerns expressed elsewhere in this survey.

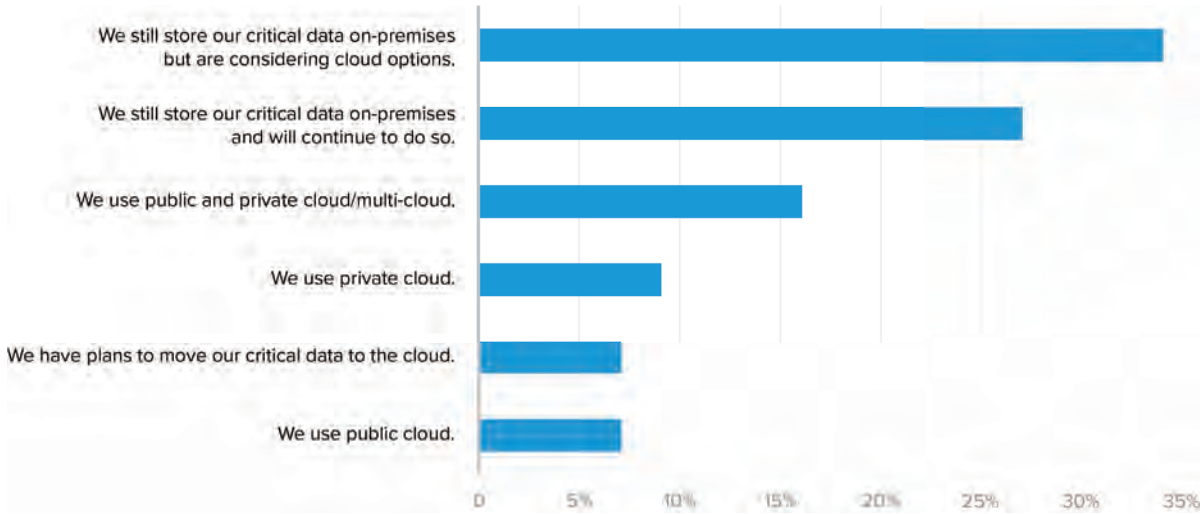
15. What is your organisation's use of cloud for fraud and financial crime solutions and data processing?



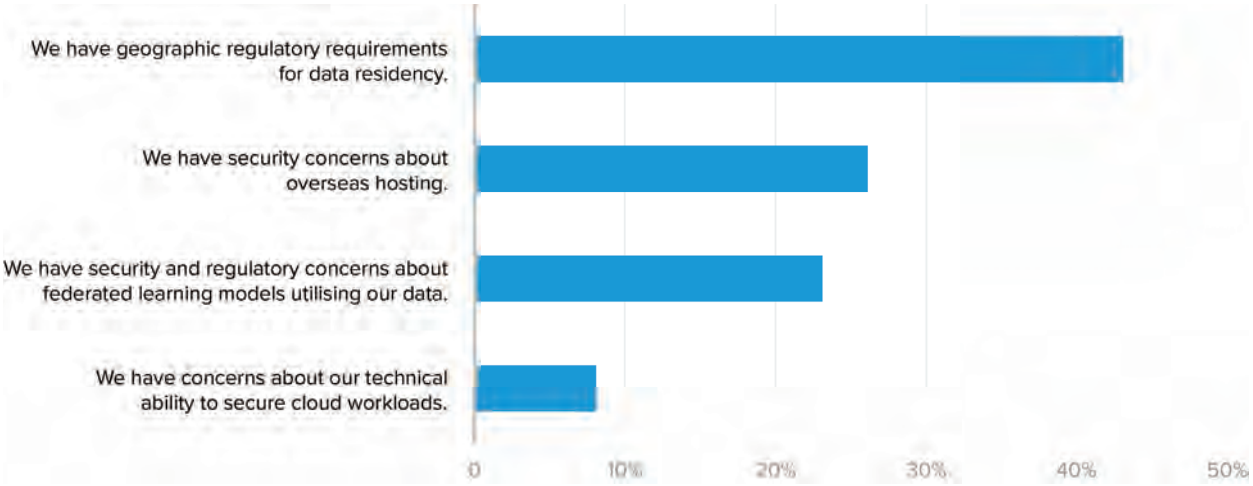
While only one-third of organisations report currently using cloud for fraud and financial crime solutions and data processing, 16% say they plan to do so, and 26% say they are assessing it.

Only 5% say they have evaluated and currently rejected this route.

16A. When considering data residency of critical data, what best describes your current approach?



16B. When considering data residency of critical data, what best describes your current concerns?



Looking at the approaches that have been adopted and the concerns around data residency of critical data, it is quickly apparent that geographic regulatory requirements for data residency remain an important factor among concerns for 43% of respondents. And 26% say they have security concerns about overseas hosting. On top of these issues, 23% have security and regulatory concerns about federated learning models using their data. A minority, 8%, say they have concerns about their technical ability to secure cloud workloads.

These factors go some way to explaining the current approach whereby 27% report that they still store critical data on-premises and will continue to do so. But a larger number, 34%, say they still store critical data on-premises but are considering cloud options.

CONCLUSIONS

In concluding this survey report, it is useful to return to some of the opening statistics shared:

- **48%** of respondents say they currently use AI/ML/analytic-based detection.
- **83%** say they will invest in other AI techniques in 2024.
- **76%** say key AI benefits include improving operational efficiency and effectiveness.
- **70%** say their biggest concern about adversarial AI is deepfakes created by attackers.

It's clear that fraud/crime fighters have spent 2023 discussing ways to employ AI in their defences, and the vast majority of them intend to unleash new investments in 2024. It is key to make these investments in light of fraud/crime trends, which include:

Top Crimes:

- Third-party-actioned compromise - 71%
- First-party-actioned scams - 51%
- Collusive activities - 37%

Top Compromise Routes:

- Email - 73%
- SMS text/instant message - 49%
- Social media - 45%

With these statistics in mind, led by survey analysis by the experts who guided this research, these conclusions emerge:

- **Build on Current Strengths for Early Wins:** As expert Ian Holmes points out, "[AI] is an umbrella term for a lot of different concepts, many of which have been used for many years." Among those is data analytics. However, Generative AI can add a new element of automation to many manual processes and augment what institutions already are doing to detect and prevent fraud and financial crime. As Holmes says, "We're happy to educate people both on how AI can help them and how it can optimise what they're doing today already with AI."
- **Build Those Use Cases:** Anomaly detection is the place to begin. As Keith Swanson of SAS emphasises, people are looking for AI to help them be more efficient and effective. "It is about: How do I focus my resources onto the highest-priority activities?" Swanson says. "They want what they're spending their time on to have highest benefit, result and outcome. It's not necessarily about AI taking over; it's more about AI targeting activities to make sure we have the best effect."
- **Keep Your Eyes on Adversaries and Regulators:** Deepfakes emerge as the top concern of survey respondents. But Holmes points out that solutions already may be at hand. "In order to prevent deepfakes, we know that biometrics can be very successful in spotting those risks that lack proof of life," yet investments in biometrics did not emerge as a top 2024 strategy. This point showcases the need for careful re-evaluation to ensure investment strategies are aligned with the evolving threatscape.

In terms of the regulatory landscape, Swanson points out rightly that "a lot of the response to how AI is applied is going to be done through a regulation lens. How are regulators going to interpret the application of it and who can use it?" This is a moving target, as administrations from the U.S., EU, China, India and elsewhere all are attempting to build regulatory guardrails around the application of AI. It is important not just to watch the regulatory developments but to help inform them through appropriate feedback loops.

In closing, the survey experts offer insight on how to embrace AI proactively:

Keith Swanson: "Key themes that came out of the survey are the role, prevalence and use of AI, but also where scams have been and where scams are going. The responses show that people are looking for pragmatism in what we need to do. We have issues we need to deal with today. We have to balance the loss, the efficiency, and regulation. It's about what are we doing as a holistic approach."

Ian Holmes: "We need to consider how AI can be nurtured because unfortunately, it's not an 'easy button.' It's just an 'easier button'. We still need guidance from a business-usage perspective in order to ensure that it is effective.

"The other area to focus on is: Once you've created AI and you know that it's effective, how do you deploy these models and operationalise their benefits into production?"

To learn more about Swanson's and Holmes's analysis of the survey results and how best to put them into production, see the Expert Analysis in the report's concluding section.

EXPERT ANALYSIS

Fighting Fraud and Financial Crime: Assessing the Impact of AI and Other Change Agents

Executive Insights on What Survey Results Mean – and How to Put Them to Work

NOTE: ISMG's Tom Field discussed the survey results with Ian Holmes – Global Director for Enterprise Fraud Solutions, SAS; Keith Swanson – Director, Risk, Fraud and Compliance, Asia-Pacific & Japan, SAS; and George Tai, Regional Sales Director Asia Pacific, Financial Services Industry - Intel. This is an excerpt of that conversation.

Standout Survey Results

TOM FIELD: What's your gut reaction to the survey results?

IAN HOLMES: Many of the respondents are actually underserving themselves, certainly around the use of AI within the banking and financial services sector. They indicate in Question 14, for example, that only 48% are currently using AI. This comes from a few areas, and one of those is certainly around the hype of what AI can be and could be to different financial institutions. It is an umbrella term for a lot of different concepts, many of which have been used for many years. This is really a rebranding of some of those areas.

It can be all the way from things like analytics and data analytics, searching of data and discovery of data. Certainly, AI brings a new flavour to that and takes some of the manual efforts out of those processes. But many of the banks are utilising AI within their fraud detection today. The regions covered by this report are doing well in that regard but if the survey is correct, then the team here we have on this webinar is going to be very busy over the next few years. And we're happy to educate people both on how AI can help them and how it can optimise what they're doing today already with AI.

KEITH SWANSON: The results highlight what we often see in practicalities when we're talking to customers: Is AI an answer looking for a problem, or do they have a problem for which they're looking for a better answer? People are really looking for artificial intelligence to drive improvements in efficiency and service additional risks. It highlights that organisations are grappling with how best to do that, that they've been dealing with the issues of ever-increasing regulation and need for resources. How do they do that balancing act?

GEORGE TAI: The velocity at which innovation is disrupting financial technology is perplexing. We are in a technology renaissance spurring limitless applications of AI in all sectors of finance.

AI is undoubtedly here to stay. As a double-edged sword, AI provides immeasurable value for the industry, but also immeasurable power for agents of nefarious intent. These results demonstrate a rapid adoption of AI, as executives face competitive risk to sustain innovation, while maintaining safety and security of their business and systems. As an industry partner, Intel designs technology with security and ethical AI as key pillars forging a root of trust in a rapidly evolving industry.

Surprises in the Survey

FIELD: What surprises you most about the findings?

HOLMES: : It's interesting that the respondents are already feeling the pressure of regulators. As we built out the questions for this report, we felt that we were looking to the future in terms of much of the changes, certainly from a fraud perspective, of how the regulators are getting involved. This was apparent within Question 13 and the responses there. That attention will really force them and their network to invest in fraud where there could be gaps today. Also, the nefarious aspects of utilising AI is a specific concern. Things like deepfakes in Question 4 is certainly top of the list there. Yet in order to prevent deepfakes, we know that biometrics can be very successful in spotting that lack of proof of life, and yet that is very low in Question 5, at only 20%.

Also, the nefarious aspects of utilising AI is a specific concern. Things like deepfakes in Question 4 is certainly top of the list there. Yet in order to prevent deepfakes, we know that biometrics can be very successful in spotting that lack of proof of life, and yet that is very low in Question 5, at only 20%.

TAI: There is a widening gap of internal and external capabilities and normalisation and availability of such capabilities is still lacking. The tenet that this survey indicates that AI technologies must further be surveyed as we are still in a bazaar of AI blackboxes that are challenging to understand. Generative AI contain over 7 billion parameters churning out results that often have accuracy concerns, despite we are in awe of the capabilities these new technologies bring forth.

Finding the right partners, system integrators, solutions vendors – is critical to assist in bringing trusted partners to provide peace of mind in a rapidly changing industry. Intel continues to work with the ecosystem and partners to ensure technology is well understood and can serve a greater purpose for end users of the financial industry.

"People are looking to AI to help them be more efficient and effective. In the past, it was system intelligence and now it's artificial intelligence. It is about: How do I focus my resources into the highest-priority activities?"

– Keith Swanson

Top AI Use Cases for Fighting Fraud

FIELD: What do you find to be the most compelling AI use cases for fighting fraud and financial crime?

HOLMES: Event scoring is a major aspect, where machine learning as a subset of artificial intelligence is applied, and this includes both supervised and unsupervised options. Supervised is where we have the ability to utilise a target field within the data in order to hone the machine learning models to be able to identify those optimally. Unsupervised is where we have less of a target or incomplete targets, and therefore we're looking for more anomalies within the data. These two aspects can be utilised in combination, depending upon the business problem we are trying to solve, or we can utilise them in isolation, depending upon if we have good data quality.

Each has its benefits, so we are able to understand how the data needs this machine learning for AI to be applicable. Also, we're seeing that it's been utilised in the optimisation of alert prioritisation in order to allow focus of the finite resources we have, but yet the ever-growing problem and therefore the workload in order to really optimise that from a fraud perspective.

SWANSON: People are looking to AI to help them be more efficient and effective. In the past, it was system intelligence, and now it's artificial intelligence. It is about: How do I focus my resources into the highest-priority activities? They want what they're spending their time on to have highest benefit, result and outcome. It's not necessarily about AI taking over; it's more about AI targeting activities to make sure we have the best effect.

Concerns About Using AI

FIELD: How can security leaders address their chief concerns about AI?

HOLMES: First, we need to consider how AI can be nurtured because unfortunately, it's not an "easy button." It's just an "easier button." We still need guidance from a business-usage perspective in order to ensure that it is effective. In areas like payments fraud, we cannot just look to the data because there are complex processes both within the industry, outside of the bank, but also from a data perspective inside of the bank. And we're

always going to get a customer or a group of customers who unfortunately spend like fraudsters. So, we need to ensure that we do not just let the AI run amok and increase the false positives or impact our customer success and customer service because that will place high pressure and burden both upon the operations we spoke about but also from a marketing perspective to ensure that they stay top of wallet.

The other area to focus on is: Once you've created AI and you know that it's effective, how do you deploy these and operationalise these into production? With the new cloud environments, we have concepts of design time and runtime in today's world. We've built the models and they're utilising AI within design time, but then we need to port it to runtime and make sure that we have consistency of data and the ability to deploy that. The other aspect is monitoring maintenance and governance of the models as we begin to utilise them. They will have a certain longevity and we hope that is a long period, but with shifts in data and in fraud trends, and depending upon the types of algorithms that are in use, the level of longevity can shift and change. We need to be able to monitor and maintain those machine learning models within the live environment.

Finally, we need to consider a multi-option strategy here. We can consider things like federated models, where we don't just have one large model, which is looking across the full scope of the data, but we break those models down into smaller models which can each focus upon a certain area. So, we could look at the payments data with the transaction amount, the beneficiary, the source, but also the date and time to get the velocity aspects. And then we could look at the channel-level models, which can be swapped out, based upon whether this is coming through the call center channel, the digital channel or even the branch channel.

"The velocity at which innovation is disrupting fintech is shocking."

– George Tai

Federated models allow us to select the relevant channel model along with the payments model in order to combine scores together and optimise that. And that breaks the problem down into smaller elements, which helps in terms of making sure that the models are as effective as possible.

SWANSON: A lot of the response to how AI is applied is going to be done through a regulation lens. How are regulators going to interpret the application of it and who can use it? We have fraud risk assessment, product risk assessment and channel risk assessment. I would not be surprised to see organisations and security leaders say, "Hey, we need an AI use [risk] assessment in which we understand how the organisation is expecting to use AI, one, in deterministic behaviours in identifying a risk, and two: What is the end outcome that is driven by AI?"

How AI Benefits Financial Institutions - And Adversaries

FIELD: What results can our respondents expect to see from use of AI in both the near and the long term? And to what degree are you seeing the adversaries employ AI now to aid their fraud and financial crime schemes?

HOLMES: Deployment of AI within financial institutions is beneficial because it helps increase all of the concepts and KPIs which they are monitored against. It increases fraud detection because of the adaptability of the AI against standard business rules in isolation. There's going to be the reduction in false positives, which is a benefit from a customer service perspective and also increases efficiency. They're going to have fewer alerts or work items,

and therefore there's going to be a reduction in resources over and above just general business rules in isolation. Some of our customers, depending upon their foundation and what we're comparing against, experience from 45% to 56% increases in benefits from a fraud detection perspective, and even higher in a reduction of false positives. There are some good case studies on our website from a fraud detection perspective that we can utilise.

Regarding the use of AI from an adversary's perspective, fraudsters are expanding their use of AI. They've been utilising concepts of AI for a long time. Bots and counterfeiting were certainly capitalising upon some of the basics of AI around 20 years ago. But now, they are using AI to take scams to the next level. They are taking the data which is available, harvesting more data directly from consumers – quite often through spam emails, spam SMS, etc. – and triangulating this with AI in order to scam and socially engineer the customers of banks even more.

"We need to ensure that we do not just let the AI run amok and increase the false positives or impact our customer success and customer service because that will place high pressure and burden both upon the operations we spoke about but also from a marketing perspective."

– Ian Holmes

Scams will become more targeted. The fraudsters will harvest even more data – maybe from our social media, from LinkedIn, etc. – in order to combine that with the data available on the dark web and also ensure that this public information is used. They will have bespoke scripts at their fingertips in order to socially engineer us as individuals, rather than a group. And the fraudsters are likely to be the first person to wish you a happy festive period, knowing that they're there to actually ruin your festive period. They will likely do that through AI-driven voice and maybe even mimicking your own family members in order to be convincing from a social engineering perspective. It really will be next-level.

TAI: As we mentioned, AI can be used for good or for nefarious purposes, a tool that accentuates the wielders' desired outcome. Intel stands strongly in seeing that technology is used to do something wonderful and the greater good. Enabling ethical AI, security, and protecting end users has always been a strong focus of intel.

Areas of Investment in Fraud Mitigation

FIELD: Where do you see institutions making new or renewed investments to fight fraud and financial crime?

SWANSON: Look at the statistics, whether from this survey or other industry bodies, around the rise of scams. Part of that goes back to the definition of scams and the nature of how scamsters are trying to manipulate situations. They're running both a wide and a deep game. It's wide in a sense in they are using multiple digital mediums and scam farms, etc. They spray and hope something hits. They make a thousand calls, send a thousand emails or thousands of texts, trying to find that weakness point. If they find it, then they're running deep with it. They use and exploit it not just in that individual compromise but again and again. Do you go down that chasing mechanism, or do organisations focus more around building a level of agility where they are able to respond much faster or where they have the right threat intelligence to proactively mitigate risks before they happen? That's where the

investment will probably happen, around building agility in responsiveness, not building just to a [singular] historical process or an exposure that might've been from a year ago.

Survey Report Takeaways

FIELD: AI aside, what are some of the other key takeaways you gleaned from the survey?

SWANSON: Key themes that came out of the survey are the role and prevalence and use of AI, but also where scams have been and where scams are going. The responses show that people are looking for pragmatism in what we need to do. We have issues we need to deal with today. We have to balance the loss, the efficiency, and regulation. It's about what are we doing as a holistic approach versus "I can't just tackle one scam type and let the others fall aside." Organisations need to look at how they can balance the exposure types they're trying to mitigate with the impacts of the techniques, data, technology, process and people they'll use to respond.

Like scams, AI is not just about how you apply it, but about the effect and the outcome. I would not be surprised if we see an assessment framework that relates back to how AI is being used, how AI affects the outcomes, and whether that falls within the organisational and regulatory frameworks in which we operate.

Putting the Findings to Use

FIELD: How do you recommend our audience put these findings to work?

SWANSON: There wasn't anything revolutionary from this. But organisations can use [the survey] as a level of consensus validation. If someone is coming to [another] and saying, "This is a one-off," or, "This isn't of issue," or, "We're not at scale yet," the survey results can help highlight that there is a systemic level of concern and a systemic level of response is needed as well. Within that, the results could be used to help drive the importance of investments being made or actions being taken, or in relation to the direction in which we need to improve. They provide a level of reinforcement of previous thoughts and a feeling of, "Hey, we all have a common challenge. Let's move forward with a common goal."

HOLMES: It's time we started to think more about the ecosystem that we all rely upon. It's currently splintered at an industry level in terms of the fraud and financial crime enforcement that we apply. Telecommunications providers, telcos, social media, email gateways, and the providers all have some responsibility in the control of scams, and these have been highlighted throughout the report. If we never received that SMS or email with the bad link, then we'd be less likely to become a target for the fraudsters.

> **"Deployment of AI in financial institutions is beneficial. Some of our customers ... experience from 45% to 56% increases in benefits from a fraud detection perspective, and even higher in a reduction of false positives."**
>
> **– Ian Holmes**

The banks, from an industry perspective, are under severe pressure to be more open. Regulators are very interested in reducing the monopolies that the banks have on the industry. Open banking is an initiative that began in the European Union, and it's spreading very quickly around the globe. Australia,

Latin America, and even the U.S. are looking at open banking as well, to just break those monopolies. The banks are often the custodians of the money, so they still have to allow access to these third parties, who are new entrants into the industry and provide services to us as customers.

Yet the regulators are not making these other payment service providers share the data back to the banks. We expect the banks to protect and reinforce the security we expect, yet they're being blinded by the data of where we are spending by these third parties, who just come and effectively take funding from within our accounts. Yes, they've authenticated the customer, etc., and they have very secure protocols to interact with the bank, but it doesn't help the bank know where I'm spending. Maybe that's not so much from a geographical perspective because a lot of these are remote channel payments, but it's the types of merchants I'm using. Does Ian Holmes normally spend at this type of merchant?

When I was spending on my bank's facilities, they would know that and they'd be able to triangulate that and profile me more effectively. But when they're blinded because of these third parties taking over the front end of the payment, it becomes very difficult for the bank to be able to assess and profile that spending, in order to be more accurate. We need to ensure that we are respective of the pressure the banks are under and that they are doing a very good job. And we need to find ways to help them to mitigate these risks, especially within the data protection regulations which are occurring, such as PDPA in Thailand, which is very close to the GDPR, which was set up in Europe.

These are all areas where the banks are really suffering, but the ecosystem needs to be there to protect them. And, yes, telcos, the email providers, etc., are all part of that.

SWANSON: In Australia, where I'm based, there's almost a daily, if not weekly, dialogue between people [customers] in the media saying, "I've lost this money because of a scam." And a few days later, one of the organisations or institutions talking about, "Here's what we're trying to do to reduce scams." The survey begs the question, "How is it we're looking outside of our internal ecosystem for additional mediums and additional collaboration, public-private partnerships to drive [better] use of data?"

> **"A key highlight in the survey is around people's use of data, or frankly, at times, lack of use of data."**
>
> **– Keith Swanson**

A key highlight in the survey is around people's use of data, or frankly, at times, lack of use of data. A lot of the different types of [scam mitigation] mediums that institutions are putting out in the media that they're trying to drive around what we are doing to reduce fraud and scams is, "We're working with the telcos to get information about scam phone numbers. We're using information from government to tell us that." It's those public-private partnerships and how you apply that information, that collective view of risk, that collective data, within the appropriate data privacy frameworks to say, "Hey, I can do better than what I can do internally, if I look outside of my organisation as to what can be contributed for a common good."

The SAS Approach

FIELD: Talk to me about SAS. How are you continuing to refine how you help your customers understand and fight both fraud and financial crime? And what should we follow up on in our next survey?

HOLMES: From a SAS perspective, it would be good to get some more details about the feature function and the fraud solutions in use within some of these financial institutions that we serve. We need to consider banks are not alone in this complex digital ecosystem, and we need to ensure that we are best placed in order to allow them to take their solutions, bring together the correct data, utilise AI machine learning, and deploy that and best protect themselves with the features and functions they have available. Maybe an alternate version of this survey could be sent to the regulators as well to see what their views are of the industry from an outside-in perspective, if they would support that. It would be very interesting, as they become even more entwined in the fraud and financial crime aspect.

And finally, we focused a lot upon external fraud. Internal fraud, unfortunately, is growing – especially as global economies begin to suffer again. The pandemic caused some increase in the internal fraud or the pressures that employees were under in order to potentially commit fraud against their employer. We need to consider how to shore up the defenses around internal fraud. There are a great deal of insights within this report. Technology, data and the application of AI machine learning are key. There's a lot of material to look at.

If they want to consider other areas, they can contact SAS. Keith and I work within a global team and there's certainly someone regionally or locally who is able to help provide additional insights and how to knit all of that together. SAS is probably, from a fraud and financial crime perspective, one of the biggest investors in subject matter expertise. We're not just there to provide you with the software, we're there to provide the wrap around that and make sure that you are best utilising the capabilities that we can offer, both from an introductory perspective but also as that goes into the future and things begin to morph and change, as they always do within fraud and financial crime.

Intel in Action

FIELD: Talk to me about Intel. How are you continuing to refine how you help your customers understand and fight both fraud and financial crime?

GEORGE TAI: Intel understands that AI is everywhere, and to enable technology that can accelerate, secure and elevate solutions is critical. Fighting fraud and financial crime, we continue to work with partners like SAS to enhance and provide as much edge as possible to ensure we provide constant value to our customers. Through our Center of Excellence in security, we hope to continue to evolve security and continue to refine and provide robustness and resilience of our security measures in our product from hardware to software to the point-to-point data transfers that occur infinite amount of times a day in financial transactions. Understanding points of failures is how we work with our partners and ensure that mindset to continuously be vigilant in how Intel and our ecosystem can drive ethical AI and support the fight against fraud and financial crime.

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 36 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.

(800) 944-0401 • sales@ismg.io

Data Breach Today
Prevention. Response. Notification.

BANK INFO SECURITY

HEALTHCARE INFO SECURITY

GOV INFO SECURITY

CAREERS INFO SECURITY

FraudToday.io

CU Just for Credit Unions INFO SECURITY

DeviceSecurity.io

PaymentSecurity.io

infoRisk TODAY

CIO.inc

CyberEd.io

CyberEdBoard

CYBER THEORY

GREYHEAD AN ISMG COMPANY

Xtra mile LIFECYCLE MARKETING

iSMG

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