Arkose Labs

New Research: The Intersection of AI, Digital Fraud and Cyber Defenses

PART 1: PURSUING AI MATURITY TO SECURE ONLINE TRANSACTIONS

November 2024

Table of Contents

Executive Summary

In today's hyper-complex digital world, the fundamental responsibility of cybersecurity and anti-fraud executives is remarkably clear: Protect your business operations, customers and employees from an increasingly hostile landscape.

High-value targets such as your revenue-generating websites and apps face expanding risks and novel threats, with account sign-ups, sign-ins, in-platform and other consumer touch points becoming the frontline for account takeovers, credential stuffing, fake account creations, etc.—often with devastating results for everyone but the bad actors.

Now AI enters the mix—machines that can learn, reason and make decisions like humans, driving innovation on both sides. Enterprises are learning to harness AI as a powerful asset, yet cybercriminals are weaponizing it for sophisticated, large-scale attacks perpetrated with AI-powered bots and human fraud farms. The real conundrum isn't if your business will be targeted by AI-powered threats, but how effectively you can deploy AI to counter these attacks that are already aiming straight at you.

> "I think that most people are underestimating just how radical the upside of AI could be, just as I think most people are underestimating how bad the risks could be." — **ANTHROPIC CHIEF EXECUTIVE OFFICER DARIO AMODEI**

In this complex environment, where essentially machines are battling machines, we sought to hear from cybersecurity executives to discern the nuances of AI and understand the pragmatic actions they are taking today and are considering taking in the near future.

As you indulge in the research findings, you'll learn why ATO/credential stuffing remains the king of concerns for roughly **3 out of 4** respondents across industries. ATO, a top attack type for decades, is only going to get harder to detect and mitigate because fraudsters have easy access to automated tools like basic and AI-powered bots and workers at fraud farms. The trend is already happening. When considering all attack activity over the past 12 months, respondents said AI-powered bots were the source for **40% of those attacks**. Attackers were very early adopters of AI because they can use it to scale attacks efficiently, which reduces their operational costs and thus improves their illicit ROI.

Other key highlights

- On average, **59%** of enterprises express serious concern about a variety of threats to their revenue-driving websites and apps.
- **Top 3** threats include account takeovers/credential stuffing, fake account creation and generative AI.
- AI is driving significant changes in attack sources, with **88%** of enterprises observing an increase in AI-powered bot attacks in the last two years.
- **61% reported higher operational costs** and declines in customer acquisition. Notably, **60% identified revenue loss** as a top negative consequence due to the threats they face.
- A majority (53%) said they have lost between **$10M to over $500M** during the past two years due to negative consequences related to cyber attacks.
- In a first, we also explored respondents' emotional state. **Execs are confident (12%)** about defending their business from volumetric AI-powered attacks, while their **teams are stressed out (12%)**.

The data points, findings and analysis are robust. This report is organized into three distinct parts, with this one focusing on the shifting risk terrain and preparedness. Part 2 explores how enterprises are using AI and reveals realized benefits of using AI to defend against adversarial AI and the expected benefits of tomorrow. Respondents shared that **21% of their cybersecurity budget** is dedicated to AI solutions today and also told us what they are expecting to spend by 2026.

Based on patterns that emerged in our analysis, we've coined and defined a new term: AI Enthusiasts. These are the enterprises that have fully embraced AI to take multiple actions to detect and mitigate attacks. Learn more from the **AI Enthusiast cohort** in Part 3 of the research dedicated specifically to this group.

The response to participate in the research was overwhelming, with nearly 200 cybersecurity professionals eager to share their insights on their pressing concerns, evolving attack patterns, and how they are harnessing solutions resistant to adversarial AI to uncover and stop online fraud. The research reveals how AI is shaping enterprises' offensive and defensive strategies today—and what they're planning for tomorrow.

We're excited to share these insights to engage you in the conversation. We invite you to set up one-on-one meetings with us to discuss your experiences so far on the AI journey.

Patrick Kehoe
CMO
p.kehoe@arkoselabs.com

Frank Teruel
CFO
f.teruel@arkoselabs.com

Vikas Shetty
Head of Product
v.shetty@arkoselabs.com

Survey Shows Most Concerning Threats

The risk terrain is shifting. As AI supercharges innovation and malicious intent at scale, cybercriminals are no longer probing the perimeter—they're infiltrating the very systems and environments that enterprises rely on for their consumers' experiences. Attacks like fake accounts, SMS toll fraud and GPT prompt compromise are evolving in scale and precision toward a singular goal: money.

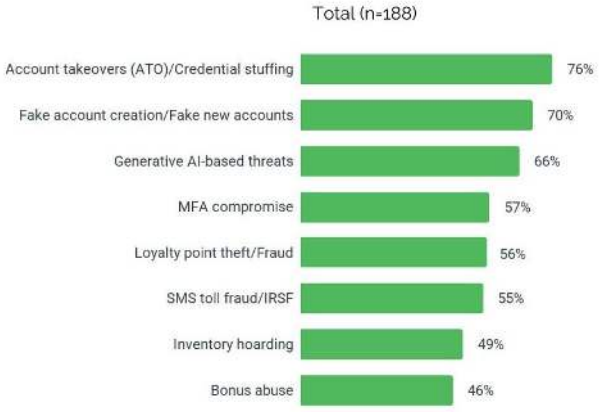
These threats assault targets at enterprises' most vulnerable entry points—the sign-in and sign-up processes—exposing critical business applications such as revenue-driving websites and apps to a constant barrage of attacks. Account takeover/ credential stuffing is still the most pressing concern, with roughly 3 out of 4 survey respondents expressing significant apprehension about its impact on their business operations and consumer experiences. For cybersecurity executives, the takeaway is clear: Trust starts the minute a consumer enters a username and password, which are the very beginning steps for today's digital consumer journey.

> "And part of what makes this really complicated is that AI facilitates attackers pivoting quickly. They think, 'hey, this attack isn't working, so I'm going to pivot to a different type and get that one done.'" — **ARKOSE LABS CFO FRANK TERUEL**

Industry Analyst firm Datos Insights recently released a survey-based report articulating its 2025 predictions. Findings corroborated research results in this report. Cybersecurity leaders at financial institutions are more concerned about adversarial AI, heading into 2025 than they were entering 2024 and the threat of account takeovers is the main risk keeping them up at night.

Level of Concern Over Threats to Critical Business Applications

Concerned to a Moderate/Large Extent



Finance (n=69)	Technology Platforms (n=33)	Travel/ Hospitality (n=35)	Social Platforms/ Networking (n=21)	Sharing/Gig Economy (n=19)	Streaming Services (n=11)
83%	79%	71%	62%	79%	55%
71%	73%	77%	62%	63%	64%
70%	76%	74%	71%	37%	36%
65%	48%	57%	71%	53%	9%
61%	48%	71%	62%	42%	9%
58%	61%	63%	33%	47%	55%
54%	55%	54%	48%	42%	9%
54%	39%	51%	24%	58%	27%

Chart 1 and Table 1

Q: Think about the critical applications to your business – such as revenue-driving apps, websites, etc. How concerned are you with each of the following threats to those critical business applications? (RATE EACH ROW)

Of the total respondents, 66% indicated they are concerned about the impact of generative AI threats. Fintechs are particularly concerned with 81% citing this as a top issue. (To see more detail on how the specific industries compare, see Table 8 in the Appendix on page 16.)

This heightened apprehension perhaps stems from fintechs' unique operational characteristics—rapid digital transactions, direct access to consumer funds and heavy reliance on APIs. These factors, coupled with a potentially less mature cybersecurity posture compared to traditional financial institutions that have a long tradition of heavy regulations, could increase fintechs' vulnerability. The real-time nature of fintech transactions, combined with the advanced automation and scalability of AI-powered attacks, make fintechs especially susceptible to sophisticated threats.

Generative AI-based threats are no longer theoretical; they are here, and they're evolving fast.

3,000% INCREASE IN AI-BASED DEEPFAKE ATTACKS BETWEEN 2022 & 2023.

Source: Hackernoon

The broad cybersecurity community, including law enforcement, is experimenting for understanding and answers. **Europol** is exploring the use of DarkLLMs to understand how they are weaponized on the dark web to identify detection methods and figure out effective actions to seize them along with their developers and users.

Our threat research unit, **ACTIR**, also has observed two new AI-related attack vectors:

1. **GPT prompt compromise:** where bots are able to programmatically submit prompts and scrape the response with an intention to either train their own models, resell similar services or gain access to proprietary, confidential and personal information.
2. **LLM platform abuse:** a vector that creates unauthorized platform replicas and uses illegal reverse proxying that copies the platform's insights.

A Thriving Threat Ecosystem: Expanding, Evolving and Lucrative

Arkose Labs' threat research unit, ACTIR, classifies financially motivated cybercriminals into three types: amateurs, professionals and mavericks. This range covers everyone from newcomers and lone-wolf attackers to organized enablers and phishing gangs. Cybercriminals now have easy access to advanced AI-powered bots and other tools used to deploy attacks like account takeovers, loyalty point fraud, MFA compromise, fake account creation, etc. Once restricted to bad actors with developer chops, advanced attack tools (plus training sessions and guides) are now widely available on the dark web, driving a surge in the frequency, severity and profitability of attacks.

Among these cyberattack enablers is *Greasy Opal*, an active group from which other bad actors can buy everything from credential-stealing software to AI-powered bots. ACTIR estimates that *Greasy Opal* earned well over $1.7 million in 2023. Alleged cybercrime-as-a-service group *Storm-1152*, which Microsoft and Arkose Labs first disrupted in December 2023 and again in August 2024, purchased AI tools from *Greasy Opal* to generate bots with human-like signatures for evasion. *Storm-1152* created (and then sold) 750 million fake Microsoft accounts. In turn, threat actor group *Scattered Spider* (credited for the 2024 MGM attack) bought many of the fake new Microsoft accounts from *Storm-1152* to further exploit them for financial gain through ransomware, etc.

This all-too-common scenario exposes today's dark web as a healthy ecosystem, drawing strength and momentum from its intertwined, sophisticated network.

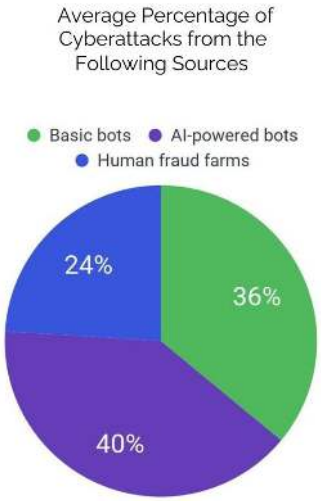
Bad Actors Commercialize AI, Causing Unprecedented Rise in Online Fraud

The commercialization of AI-powered tools, like bots, demonstrates the growing sophistication and scale of attacks, as well as highlights the democratization of attacks contributing to the rapid evolution of the threat landscape. As bad actors refine their tactics, techniques and procedures, enterprises must be equally agile in their defenses.

This need for agility is underscored by findings from participants in this research, which reveal that AI-powered bots were the most common source of cyberattacks over the past 12 months. These bots are the tools that bad actors easily buy from dark web markets and then deploy to perpetrate account takeovers, register hundreds of thousands of fake accounts, compromise defenses like MFA, etc.

Such attacks have grown in frequency for the vast majority of companies over the past two years. Basic bots and human fraud farms, which tend to be low and slow, are tracking in lock step with AI-powered bots and have also largely increased over the past two years.

> "The scale of fraud threats and techniques is really escalating, especially with fraud as a service taking off. It's becoming more dangerous every year, and in just a year or two, we could see an exponential spike. That's why we think it's crucial to fight fire with fire. The bad guys are leveraging AI, so we have to be at least as adept, if not better, with our AI defenses." — **SENIOR EXECUTIVE, DIGITAL PRODUCT MANAGEMENT, FINANCIAL SERVICES INDUSTRY**



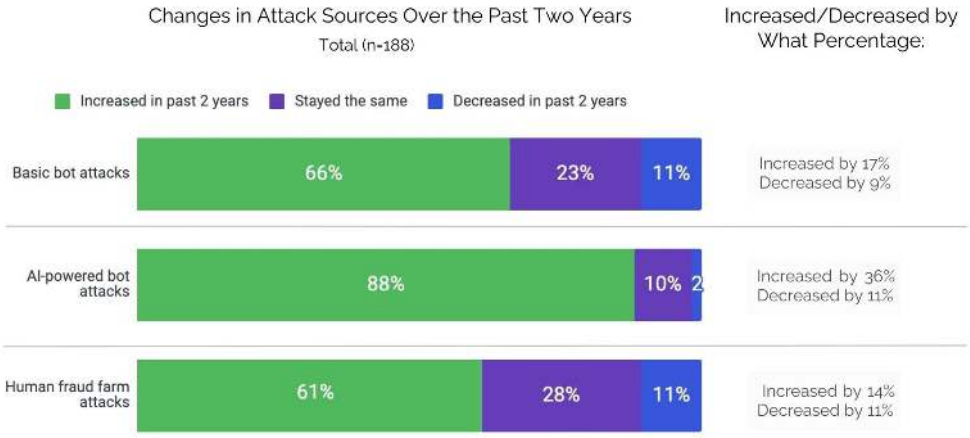


Chart 2 and Chart 3

Q: With all the attack activity your company has seen over the past 12 months, approximately what percentage of those attacks were from basic bots, AI-powered bots and human fraud farms? Provide your best approximation.`

Q: And estimate to the best of your knowledge how those attack percentages have changed from 2 years ago.

Digital Siege: The Unseen War on an AI Innovator

A prominent company specializing in large language models (LLMs) encountered an unprecedented crisis. A wave of bot-driven cyberattacks was threatening its operations, costing millions and straining resources.

The crisis erupted with over 2 billion bot incursions in a matter of months. Approximately 4-5% of the millions of daily prompts were flagged as suspicious, leading to significant losses. Attackers were exploiting the company's platform, proxying LLMs to bypass API fees and sell unauthorized subscriptions. Despite its efforts, the company's security measures proved insufficient, incurring heavy costs. It turned to Arkose Labs for help.

Arkose Labs offered the company a comprehensive strategy to restore order while ensuring a seamless user experience. Arkose Labs initially targeted fake account creations and SMS toll fraud. Then, when attackers shifted to chat prompts, Arkose Labs countered with advanced defenses, including AI-resistant challenges.

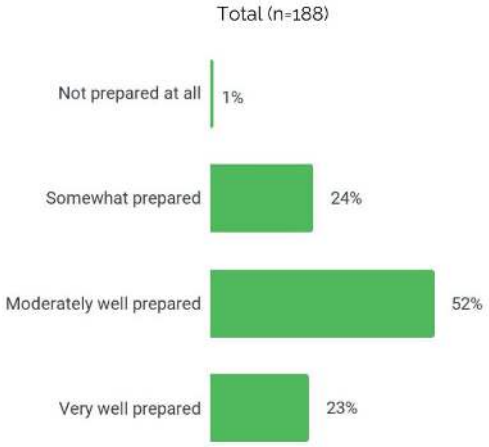
The tide turned. Arkose Labs' strategies shut down hacker repositories and forced many attackers to abandon their schemes. A brief deactivation of the Arkose Labs solutions led to catastrophic volumetric attacks, overwhelming systems and necessitating immediate reinstatement. The end results? A 99% reduction in LLM platform abuse and protection of hundreds of millions in resources. This narrative serves as a stark reminder of the lengths cybercriminals will go to, emphasizing the need for vigilance against automated attacks.

The Path to AI Maturity: Enterprise Preparedness

The harsh reality is that while cybercriminals are well-prepared to launch AI-powered attacks, most enterprises are playing catch-up. Only 23% of respondents consider themselves very well prepared to defend against these threats. In the banking sector, that figure drops to 19%, and in industries like airlines and hotels, it's as low as 14%.

This lack of preparedness is a significant concern, especially when considering the pace at which cybercriminals innovate. Enterprises must close this gap to avoid falling further behind.

Level of Preparedness for Defending Against Bad Actors Conducting Volumetric AI-Powered Attacks



Finance (n=69)	Technology Platforms (n=33)	Travel/Hospitality (n=35)	Social Platforms/ Networking (n=21)	Sharing/Gig Economy (n=19)	Streaming Services (n=11)
0%	3%	0%	0%	0%	0%
30%	18%	23%	14%	21%	27%
41%	42%	63%	67%	63%	73%
29%	36%	14%	19%	16%	0%

Chart 4 and Table 2

Q. How prepared would you rate your company in terms of defending against bad actors conducting volumetric attacks using AI-powered bots? (SELECT ONE)

Emotional Preparedness: It Depends

It's not just technical preparedness that matters—emotional preparedness is also crucial. When it comes to volumetric AI-powered attacks on companies, stress and confidence are the most commonly felt emotions.

When asked which emotions they most associate with AI-powered attacks, responses revealed a disconnect between executive confidence and the stress felt by teams directly handling these threats. Senior executive leadership feels confident (12%) about defending against volumetric AI-powered attacks, but people at the director and manager levels are feeling stressed (12%).

Many global enterprises across industries are leveraging managed services to alleviate stress that directors and managers are experiencing due to the surge in volumetric AI-powered attacks.

Emotions Associated with AI When Considering Volumetric AI-Powered Attacks on Companies

Interpretive Note: Percentages indicate relative associations. As an example, ***Stress* is 2X more commonly associated** with volumetric AI-powered attacks on companies than *Contentment*.

Chart 5

Top 3 Emotions for Financial Services Industry (n=60)
1. Confidence (12%)
2. Peace of Mind (11%)
3. Excitement (10%)

Table 3

Top Emotion by Title (n=157)	
C-suite/VPs (n=47):	**Directors/Managers (n=110):**
Confidence (12%)	Stress (12%)

Table 4

Increased Sophistication and Frequency Amidst a Talent Shortage

AI presents a double-edged sword for enterprises. While it heightens the sophistication and frequency of cyberattacks and online fraud, it is also becoming indispensable for defense. Over half (56%) of enterprises acknowledge that generative AI has intensified these challenges, putting increased pressure on cybersecurity and fraud teams. Compounding this reality is a significant skills gap—51% of enterprises report a shortage of personnel with AI plus cybersecurity expertise.

Generative AI has significantly lowered barriers for malicious actors, enabling them to execute complex attacks by enhancing traditional techniques such as scraping and phishing with advanced AI tools. The progression towards Large Action Models (LAM) and the increasing integration of AI-powered workflows, such as Chat Assistants, have expanded the landscape for potential cyber threats. As enterprises continue migrating core operations to AI-driven platforms, these systems are becoming high-priority targets for sophisticated cyberattacks.

Cybersecurity executives are now tasked with bridging a growing skills gap that includes both cybersecurity and AI competencies. Over the last year, job postings in cybersecurity that require AI skills rose from 6.3% to 9.6%.

The skills problem is even more acute in certain sectors like airlines, where 71% face talent shortages.

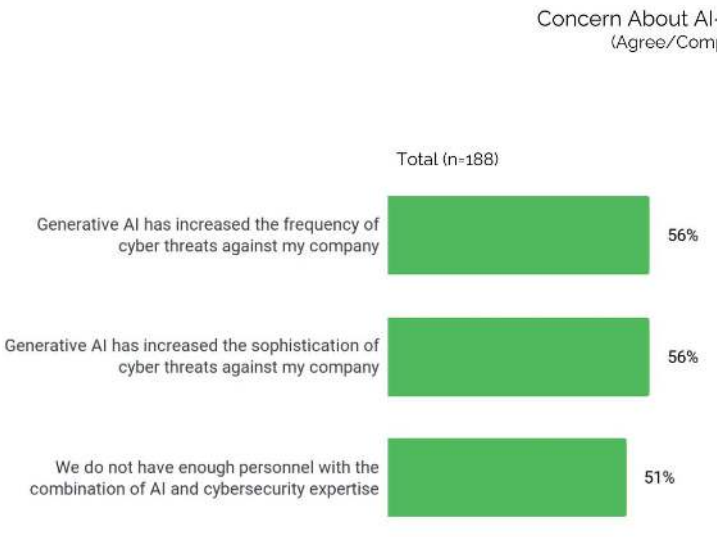
This gap highlights a critical challenge on the path to AI maturity to detect and stop threats like account takeovers, fake account creation, MFA compromise, SMS toll fraud, etc. While enterprises recognize the shifting attack landscape driven by AI, especially generative AI, many lack the in-house skills to counter it.

Interestingly, in Part 2 of this research you'll learn 62% of respondents reveal they derive greater value from purchasing AI-powered cybersecurity solutions than building them in-house. And again, the airline industry stands out with 71% indicating that they are buying versus building AI-powered solutions. This reliance on external vendors suggests that many enterprises are addressing the skills gap by partnering with cybersecurity vendors who already have AI-driven defenses, alleviating immediate pressure on internal teams to develop dual expertise.

A direct correlation exists between the increase in attack frequency and sophistication and the increase in attack ROI. Financially motivated attackers are smart business people. If an attack on a global bank, for example, doesn't yield a high ROI they move on to less protected targets. Leading enterprises are actively investing in tools that sabotage attacker ROI to hit them where it hurts most - their digital wallets.

> "My partners (I'm a programmer) lost time and money while **ArkoseLabs** (funcaptcha) introduced new precautions on Twitter," Quotpw wrote in a Telegram reply.

Image 1: *Krebs on Security article titled Interview with a Crypto Scam Investment Spammer*



	Finance (n=69)	Technology Platforms (n=33)	Travel/ Hospitality (n=35)	Social Platforms/ Networking (n=21)	Sharing/ Gig Economy (n=19)	Streaming Services (n=11)
Generative AI has increased the frequency of cyber threats against my company	52%	58%	60%	52%	63%	64%
Generative AI has increased the sophistication of cyber threats against my company	58%	55%	49%	67%	63%	45%
We do not have enough personnel with the combination of AI and cybersecurity expertise	46%	52%	54%	62%	53%	36%

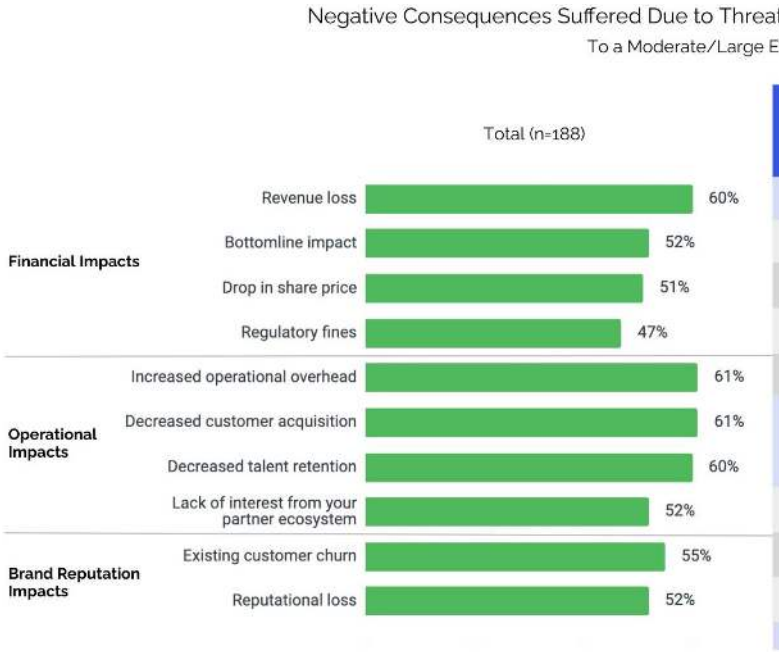
Chart 6 and Table 5

Q. How much do you agree with each of the following AI-related cybersecurity statements… (RANDOMIZE; RATE EACH)

For a more detailed view, by industry, of companies that report not having enough personnel with the combination of AI and cybersecurity expertise, please see Table 9 in the Appendix on page 16.

The Business Cost of Not Being Prepared

The high concern reflected in the threats listed on Chart 1 is warranted, as the consequences of failing to address these threats are severe. The research shows that 60% of companies experienced revenue loss, while 61% faced higher operational overhead. Customer trust has also suffered: 61% of companies reported drops in customer acquisition, and 55% saw customer churn directly resulting from these cyber incidents. Combined, all of these negative consequences are interrelated and ultimately impact business operations and profitable growth.



	Finance (n=69)	Technology Platforms (n=33)	Travel/ Hospitality (n=35)	Social Platforms/ Networking (n=21)	Sharing/ Gig Economy (n=19)	Streaming Services (n=11)
Revenue loss	65%	64%	60%	52%	47%	55%
Bottomline impact	57%	55%	49%	52%	53%	27%
Drop in share price	59%	45%	57%	38%	47%	18%
Regulatory fines	51%	48%	54%	29%	47%	36%
Increased operational overhead	58%	73%	66%	57%	58%	45%
Decreased customer acquisition	64%	45%	69%	62%	63%	64%
Decreased talent retention	61%	48%	57%	48%	89%	64%
Lack of interest from your partner ecosystem	55%	55%	54%	52%	37%	36%
Existing customer churn	59%	58%	49%	43%	63%	55%
Reputational loss	59%	45%	54%	43%	47%	36%

Top 3 negative consequences for each industry highlighted

Chart 7 and Table 6

Q. To what extent has your organization suffered negative consequences over the last 2 years in each of the following areas due to the threats just considered? (RANDOMIZE; RATE EACH ROW)

In specific industries the results are even more telling, and the negative financial consequences over the past two years are staggering. For a more detailed view, by industry, please see table 10 in the Appendix on page 17.

Among the enterprises surveyed, 53% reported losses between $10M to over $500M during the past two years due to the negative consequences related to the cyber threats listed in Chart 1.

- **Smaller companies ($100M–$499M)** report lower absolute losses, primarily under $10M.
- **Mid-sized companies ($500M–$5B)** experience a wider range, with some seeing losses up to $500M.
- **Large companies ($5B+)** often report substantial losses, with many of the largest firms experiencing losses over $100M.

To see a more detailed view of this data, please see Table 11 in the Appendix on page 18.

These numbers illustrate that inaction—or insufficient action—has a real and measurable cost. Furthermore, we expect that cost to increase exponentially due to the increase in the number of active attackers and the ease of access on the dark web to powerful attack tools like AI-powered bots.

Approximate Cost of Negative Consequences From Threats to Critical Business Applications

	Finance (n=69)	Technology Platforms (n=33)	Travel/Hospitality (n=35)	Social Platforms/ Networking (n=21)	Sharing/Gig Economy (n=19)	Streaming Services (n=11)
Less than $1M	7%	15%	9%	14%	16%	0%
$1M to $9.9M	30%	33%	46%	57%	37%	27%
$10M to $99M	45%	33%	31%	29%	42%	64%
$100M to $500M	12%	15%	9%	0%	5%	9%
Over $500M	6%	3%	6%	0%	0%	0%

Chart 8 and Table 7
Q: And what is the approximate DOLLAR quantification of these consequences over the past 2 years… that is, how much have these negative consequences COST your business to the best of your knowledge? (SELECT ONE)

Best Practices for Bolstering Your Defenses Against AI-Powered Attacks, by Use Case

Implementing preemptive defenses at the consumer level is crucial for enhancing security, enabling your business to proactively detect and mitigate risk. Below are best practices for consideration and conversation.

USE CASE	BEST PRACTICE 1	BEST PRACTICE 2
Account takeover/ credential stuffing	Use a blend of real-time, dynamic, previously unseen challenges—both visible and non-visible—to validate user authenticity and enable good user throughput.	Leverage AI-resistant challenges that cannot be detected by adversarial AI tools.
MFA compromise	Enable real-time identification of reverse-proxy phishing sites during consumer login.	Activate real-time alerts to enable immediate fraud mitigation as incidents occur.
Generative AI threats	Ensure robust detection and mitigation are in place around bad bots and all types of scrapers.	Identify reverse-proxy phishing sites that attempt to bypass geographical restrictions and impersonate legitimate users.
SMS toll fraud	Leverage detection that can quickly flag registration abandonment.	Establish baseline benchmarks for normal SMS spending and rapidly measure and analyze these metrics.

Recommendations

1. Focus first on the top threats that are putting enterprises most at risk: ATO/credential stuffing, fake account creation and generative AI. Stop potential fraud at the beginning of the consumer experience: sign-up and sign-in.
2. Challenge any workflows that bypass security measures, as they can create vulnerabilities, and incorporate dynamic elements to prevent AI models from adapting or learning from them. Regularly revisit these processes to ensure they align with your security protocols.
3. Prioritize and leverage solution providers who provide cross-industry risk signals that you can leverage to tune your internal cyber risk and fraud AI models.
4. Enhance your approach to accounts that are linked (e.g., linked bank accounts, linked loyalty accounts) by implementing rigorous verification processes. When linking accounts, always challenge the originating account to mitigate risks of fraud, particularly from new or unverified accounts, with a blend of dynamic, visible and non-visible challenges to foil adversarial AI.
5. Conduct due diligence to ensure your partners have the necessary skills to combat emerging threats and keep you well informed on emerging attack shifts by providing risk signals and threat intelligence that cover the fastest growing attack sources, AI-powered bots and human fraud farms.
6. Reduce AI risks and downstream costs by partnering with a vendor that has successful deployments of AI-resistant solutions at enterprises you consider your peers.
7. Touch base with your team regularly to understand the stress levels they are experiencing due to the rise in AI threats on your company.
8. Prioritize the use of third-party solutions over homegrown solutions, given most enterprises will most likely not be able to build solutions that are able to surpass the two-year+ head start most bad actors already have and stay at the cutting edge of generative AI-powered attacks.

> "We are at the forefront of an AI-empowered world, but we must work together to outmatch our adversaries." — **TOM BURT, CORPORATE VICE PRESIDENT, CUSTOMER SECURITY & TRUST, MICROSOFT**

Conclusion

Bad actors have been swift adopters of AI. Groups like *Storm-1152*, after being disrupted by the Arkose Labs threat research group and Microsoft's DCU, rapidly reconstituted and advanced their use of AI to create sophisticated attack signatures that challenge traditional detection methods. Free from ethical constraints and regulatory hurdles, their agility gives cybercriminals a dangerous advantage. As Datos Insights Chief Insights Officer Julie Conroy highlights, bad actors don't face the same compliance challenges as enterprises, allowing them to innovate rapidly in deploying AI-powered attacks.

For enterprises, AI presents a risk and an opportunity. The critical question: How prepared is your organization to deploy AI-resistant solutions?

To stay ahead, enterprises must act as swiftly as their adversaries in leveraging AI for defense. Given the current skills gap, a dark web economy thriving on selling ready-made AI-powered attack tools and the rapid evolution of threats, the most effective quick-start strategy is to partner with trusted vendors offering solutions that are resistant to adversarial AI security solutions, rather than waiting to build in-house capabilities or source scarce talent.

Part 2 of the research delves into how various industries are putting AI into action, while Part 3 highlights the AI enthusiasts leading successful deployments at large companies.

Methodology

The new research "The Intersection of AI, Online Fraud and Cyber Defenses" assesses market awareness and strategic deployment of AI in defensive and offensive applications. It focuses on key sectors such as financial services (banks and fintechs), social media, sharing/gig economy, streaming services, travel and hospitality (airlines and hotels) and large technology platforms. The research examines how enterprises are using AI to enhance security protocols and counter emerging threats, as well as how they are experiencing bad actors deploying AI, including bots and fraud farms, to carry out cyberattacks and online fraud.

Survey Design and Execution

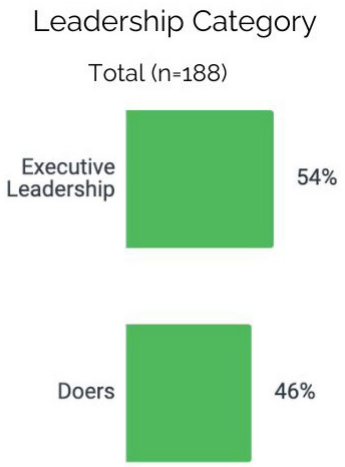
A 15-minute, close-ended online survey was conducted from September 3 to 23, 2024, targeting 188 U.S.-based cybersecurity professionals. The sample pool focused on enterprise-sized companies, with 80% of respondents working at firms where annual revenue ranged between $500 million to $10 billion or more. Participants included 54% executives (C-suite and VP-level) and 46% directors/managers, ensuring a mix of strategic and operational insights.

The primary goals of this research are to:

- Provide data-driven insights to assess the maturity of AI adoption in defensive cybersecurity measures.
- Gauge awareness of threats posed by malicious actors.
- Identify gaps and opportunities in enterprises' AI maturity.
- Identify best practices and actions companies are using today.
- Recommend mitigants to AI-powered risks and threats.

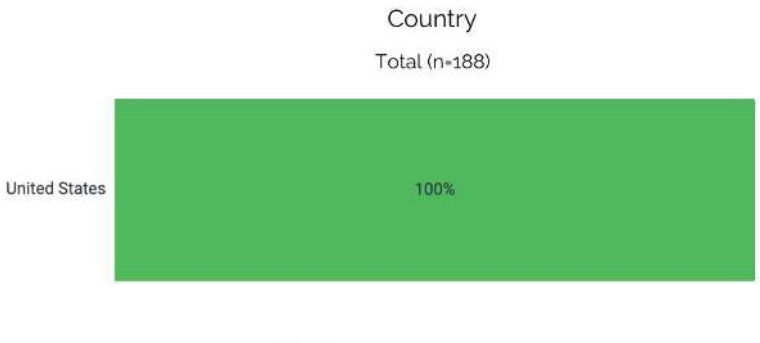
Demographics

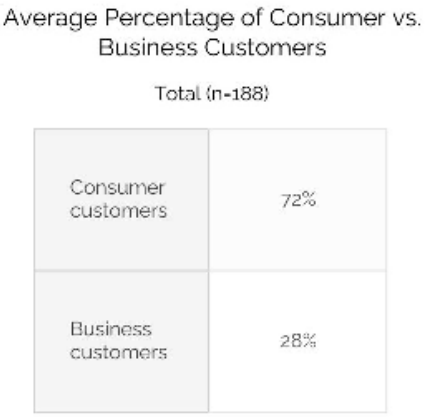
Details of the professionals who participated in the research project.

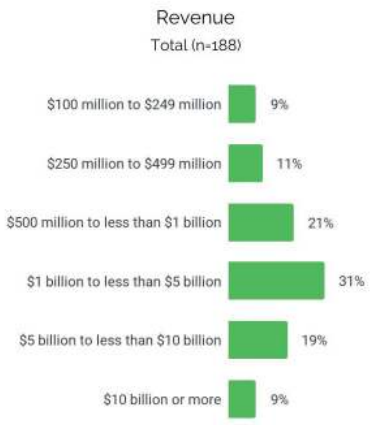


Firmographics

Details of the enterprises that participated in the research project.







Contact

For the world's leading brands, Arkose Labs delivers real-time digital risk intelligence to ensure a seamless experience for legitimate users and enhance internal cybersecurity and fraud models. Arkose Labs protects against account takeovers, fake account creation, MFA compromise and other attacks from bots and bad actors before they make impact. **Book your demo today.**

Patrick Kehoe
CMO
p.kehoe@arkoselabs.com

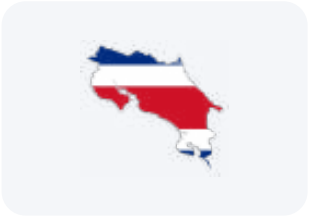
Frank Teruel
CFO
f.teruel@arkoselabs.com

Vikas Shetty
Head of Product
v.shetty@arkoselabs.com

USA
400 Concar Dr. Fl 4
San Mateo, CA 94403

Australia
T.C. Beirne Building, 315 Brunswick Street (level 4), Fortitude Valley, Brisbane QLD 4006

UK
167-169 Great Portland Street, 5th Floor, London, W1W 5PF



Costa Rica
WeWork c/o Alina Mora
Calle 118B San Rafael
San José, SJ 1020

India
Redbrick Offices,
Tower B 2nd Floor,
Panchshil Business Park
Balewadi High Street,
Off, Baner – Balewadi Rd,
Pune, Maharashtra 411045

Argentina
Avenida Corrientes 800,
Buenos Aires,
Buenos Aires C1008

Appendix: Industry Data Tables

This appendix presents essential tables that provide detailed industry insights into the survey data discussed throughout Part 1. These tables expand on the findings related to generative AI threats and industry-specific personnel shortages in cybersecurity and AI expertise.

Table 8 is an expansion of Chart 1 and Table 1 on page 5 and shows how the specific industries compare regarding their concern about the impact of generative AI threats.

Top 2 boxes ("To a Moderate / Large Extent")	Total	Banks	Fintechs	Social Media/ Networking	Technology Platforms	Airlines	Hotels	Sharing/Gig Economy	Streaming Services
Total	188	42	27	21	33	7	28	19	11
Generative AI-based threats	66%	62%	81%	71%	76%	71%	75%	37%	36%

Q: Think about the critical applications to your business – such as revenue-driving apps, websites, etc. How concerned are you with each of the following threats to those critical business applications? (RATE EACH ROW)

Table 9 is an expansion of Chart 6 and Table 5 on page 10 and shows the percent, by industry, of companies that report not having enough personnel with the combination of AI and cybersecurity expertise.

Top 2 boxes ("Agree/ Completely agree")	Total	Banks	Fintechs	Social Media/ Networking	Technology Platforms	Airlines	Hotels	Sharing/Gig Economy	Streaming Services
Total	188	42	27	21	33	7	28	19	11
We do not have enough personnel with the combination of AI and cybersecurity expertise	51%	48%	44%	62%	52%	71%	50%	53%	36%

Q: And how much do you agree with each of the following AI-related cybersecurity statements… (RANDOMIZE; RATE EACH)

Appendix: Industry Data Tables

Table 10 is an expansion of Chart 7 and Table 6 on page 10 and shows, by industry, the negative consequences suffered due to threats to critical business applications.

Top 2 boxes ("To a Moderate/ Large Extent")	Total	Banks	Fintechs	Social Media/ Networking	Technology Platforms	Airlines	Hotels	Sharing/Gig Economy	Streaming Services
Total	188	42	27	21	33	7	28	19	11
Revenue loss	60%	64%	67%	52%	64%	71%	57%	47%	55%
Bottom line impact	52%	52%	63%	52%	55%	29%	54%	53%	27%
Regulatory fines	47%	50%	52%	29%	48%	43%	57%	47%	36%
Drop in share price	51%	52%	70%	38%	45%	57%	57%	47%	18%
Increased operational overhead	61%	64%	48%	57%	73%	57%	68%	58%	45%
Lack of interest from your partner ecosystem	52%	50%	63%	52%	55%	71%	50%	37%	36%
Decreased talent retention	60%	64%	56%	48%	48%	57%	57%	89%	64%
Decreased customer acquisition	61%	64%	63%	62%	45%	57%	71%	63%	64%
Reputational loss	52%	62%	56%	43%	45%	86%	46%	47%	36%
Existing customer churn	55%	62%	56%	43%	58%	43%	50%	63%	55%

Q: To what extent has your organization suffered negative consequences over the last 2 years in each of the following areas due to the threats just considered? (RANDOMIZE; RATE EACH ROW)

Appendix: Industry Data Tables

Table 11 is an expansion of the data presented on page 11 and shows a detailed view of reported losses, by enterprise size, due to the negative consequences related to the cyber threats listed in Chart 1.

		Approximate Loss Caused by Cyber Threats Over Two-Year Period				
		Less than $1M	$1M to $9.9M	$10M to $99M	$100M to $500M	Over $500M
Approximate Annual Company Revenue	Less than $100M	0%	0%	0%	0%	0%
	$100M to $249M	11%	14%	5%	6%	0%
	$250M to $499M	11%	16%	9%	6%	0%
	$500M to less than $1B	58%	20%	16%	6%	14%
	$1B to less than $5B	16%	30%	36%	33%	29%
	$5B to less than $10B	0%	20%	27%	11%	0%
	$10B or more	5%	0%	5%	39%	57%

Q: What was the approximate annual revenue for your organization (in USD) for your most recent fiscal year? [1]

Q: What is the approximate DOLLAR quantification of these consequences over the past 2 years... that is, how much have these negative consequences COST your business to the best of your knowledge?