Arkose Labs

2023 CYBERCRIME PREVENTION PLAYBOOK

How to navigate the evolving threats of today

- THE EVOLVING **LANDSCAPE**
- BUSINESS **PREPAREDNESS**
- ACTION **CHECKLIST**
- 2023 ATTACK **MANIFESTO**

A MANIFESTO FOR STOPPING CYBERATTACK

> We can only see a short distance ahead, but we can see plenty there that needs to be done.
> *-Alan Turing*

Although the pandemic is mostly in the rearview window, many aspects of the business world have been forever altered. As a result of the global shutdown, organizations have been forced to adapt to unique circumstances and a predominantly digital environment. And as businesses are making these changes, bad actors are following them every step of the way.

Projections for 2023 and beyond show one thing for certain—without urgent action, online attacks, including Cybercrime-as-a-service (CaaS), will evolve to be more efficient and profitable than ever. To stem the rising tide, businesses need to assume a zero-tolerance approach that addresses the root causes of online crime. This move requires a clear understanding of the financial incentives and implications of attacks. Due to CaaS, cybercriminals have easy access to a complex ecosystem of tools and entities to help them commit attacks at scale while maximizing their profits.

The nature of cyberattacks is constantly changing, with bad actors designing increasingly creative approaches. To combat this reality, internal fraud and security teams must be equally innovative, viewing attack prevention not as an obstacle, but as an essential driver for long-term growth and cost savings.

The overall state of security must be achieved without impacting the experience of legitimate users. You can have the greatest security defenses in the world, but if they also stop your real customers from accessing your site, they are worthless. Balancing attack prevention with a protected user experience is a fine line that digital businesses need to walk.

So, what is the best way to maximize your ROI while preventing cybercrime from hurting your business in 2023?

Arkose Labs

2023 ATTACK MANIFESTO

FINDING SECURITY IN AN EVOLVING THREAT LANDSCAPE

1 CYBERCRIME ECOSYSTEM:

Online attacks are not created in a vacuum. Every cyber threat is the direct product of a highly interconnected ecosystem. Understanding how bad actors utilize this ecosystem (and how you can undermine their success) is the key to stopping cyberattacks.

2 MONEY BEHIND ATTACKS:

No one launches a cyberattack just for fun. Cybercriminals are highly motivated to make money, which means drastically reducing their potential ROI from an attack is what stops their ambition to launch them in the first place.

3 A RANGE OF DIGITAL TOUCHPOINTS:

Threats today are mounted and launched across a multitude of digital touchpoints using intelligent bots, humans, or a mixture of both—across a multitude of digital touchpoints. Understanding all the different attack types and the nuances behind each one empowers businesses to identify and prevent abuse on their platform.

4 STRATEGIC FOCUS ON SECURITY:

Cybercrime is not typically considered a strategic driver of business growth, but it should be. Successful businesses will put a strategic focus on fraud and security, realizing they are imperative to driving revenue, creating loyal customers, and delivering better ROI.

5 BALANCED PROTECTION:

Attack prevention is a balancing act between creating resistance that frustrates the efforts of bad actors and protecting the good user experience. User-centric security measures are the key to success, but beware of uber-lax approaches, as they will spur on future attacks.

01

DEFENDING AGAINST AN INTERCONNECTED CYBERCRIME ECOSYSTEM

THE EVOLVING LANDSCAPE

Cybercrime is like any other job—people wake up each day and go to work to make money, often virtually. For cybercriminals, the ROI for attacks must be worth it. They have to make more money from the attack itself than what they spent launching it. With a global ecosystem enabling the profitability of attacks, bad actors are now working with a comprehensive set of shadow services—all of which enable them to tap the resources necessary to carry out attacks at scale while learning new strategies.

The one constant in the fight against cyberattack is perpetual change. As a result of the interconnected cybercrime ecosystem, the techniques, tactics, and strategies used to commit fraud are always evolving. Attackers have a constant stream of fresh data and fresh tools with which to attack businesses. They are able to share successful attack techniques and iterate on one another's approaches, both of which bolster their efficacy and success.

BUSINESS PREPAREDNESS

Businesses are increasingly recognizing the importance of cybersecurity and are making efforts to prepare for the evolving online attack landscape. However, many businesses continue to fall short when it comes to implementing comprehensive security measures. Companies should invest in employee training around best practices, create strong passwords, enable two-factor authentication, and develop an incident response plan that is regularly reviewed and updated.

Businesses today also need to engage the services of a trusted third-party security consultant to assess their current security posture and identify any potential vulnerabilities—and ensure their systems and data are backed up regularly and stored offsite. This move allows organizations to recover quickly from a successful attack and reduce the financial impact. Through these steps, businesses can better prepare for potential cyber threats and reduce the risk of becoming a victim of an attack.

ACCOUNT REGISTRATION

Fake Account Registration | Credential Testing | Bonus Abuse

ACCOUNT PROTECTION

Credential Stuffing | Account Takeover | Payments | Loyalty Points

SPAM & ABUSE

Inventory Hoarding | Scraping | In-Game Abuse | Fake Reviews | Spam

PROTECTING FULL CUSTOMER JOURNEY

DEKSTOP

CONSOLES & SMART TVS

MOBILE

ACTION CHECKLIST

- Analyze all customer interaction points to discover potential avenues of revenue-generating opportunities for attackers.
- Focus on creating solutions that are compatible with all consumer devices and provide a consistent experience across all channels.
- Build your defenses under the assumption that cheap, stolen data is being used at scale to attack using both automation and human "guns for hire."
- Collaborate closely via industry groups, consortium and vendor user groups to play an active role in the anti-cybercrime ecosystem and share key information.

02

UNDERMINING THE INCENTIVE OF CYBERCRIME

THE EVOLVING LANDSCAPE

Cybercrime is now a huge, multinational business that targets all sectors. It is powered by complex networks of highly skilled bad actors, click farms, and bad bots. This business must be viewed like any other, with profit as the main motivator.

The direct victims of these attacks include businesses and their customers, but the wider consequences are more sinister. The proceeds of these attacks act as a major funding stream for serious organized crime, including the drug trade, human trafficking, and major terrorist attacks.

SPOTLIGHT ON CYBERCRIME-AS-A-SERVICE (CAAS)

Cybercrime as a Service (CaaS) is an emerging trend in which cybercriminals are offering their services to other malicious actors. This type of cybercrime is becoming increasingly common, impacting all sorts of online businesses. CaaS allows malicious actors to purchase access to compromised or vulnerable systems, or rent out services such as malware, ransomware, and DDoS attacks. Cybercriminal groups are using CaaS to efficiently and effectively target vulnerable networks and systems, allowing them to steal data, disrupt services, and extort money from businesses.

The rise of CaaS has caused an increase in the number of cyber incidents and breaches, resulting in significant financial and reputational damage to businesses. The proliferation of CaaS has also made it easier for threat actors to launch successful attacks and to quickly spread their malicious activaities to a wider range of targets. Organizations must have effective security measures in place to protect against the threat of CaaS. These measures include:

- Regularly patching and updating software and systems
- Implementing strong access controls
- Encrypting sensitive data
- Monitoring for suspicious activity

Additionally, organizations should be aware of potential indicators of compromise and regularly audit their networks and systems to identify potential weaknesses or vulnerabilities that could be exploited by attackers. Finally, businesses must ensure that their employees are trained and knowledgeable about cyber threats and security best practices. By taking proactive steps to protect against CaaS, organizations can reduce their risk of becoming the next digital victim.

STATS:

- CaaS caused $6 trillion in damages in 2022 alone.
- Experts predict some 33 billion accounts will be breached through CaaS-driven attacks in 2023.

MONEY BEHIND ATTACKS

The low-cost, high-reward cybercrime ecosystem is based on multiple global socio-economic and technological factors. To begin with, regions with low costs of living and weak currencies incentivize individuals to launch attacks against U.S. businesses, as they can reap greater rewards with the same effort they would expend in other parts of the world.

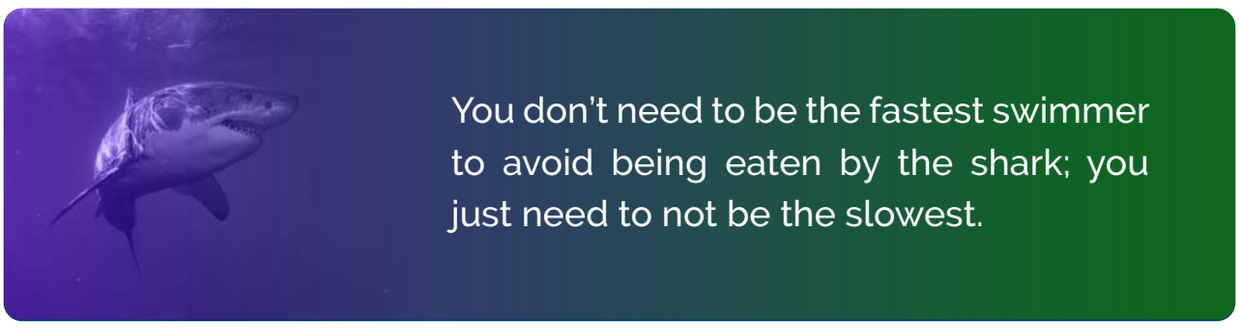
In addition to this, access to the technology necessary to launch attacks is also a major contributor. Countries with high internet penetration rates are more likely to become major sources of virtual crime, as individuals in these areas have more opportunities to access the resources and expertise needed to commit cybercrime. It is true, cybercriminals can easily collaborate with one another in these regions, enabling them to launch more advanced attacks.

The key to bankrupting an attacker's ROI is to understand their motives, capabilities, and methods. It is important to recognize that while some attackers may have technical knowledge, their primary strength lies in their ability to find and exploit vulnerable networks and resources. The most successful criminals are adept at manipulating people, systems, and networks to carry out sophisticated malicious campaigns.

To truly bankrupt an attacker, organizations must gain insight into their operations, networks, and resources. This can include comprehensive security analysis, threat intelligence gathering, and incident response. By gaining a better understanding of the adversary, organizations can more effectively identify and respond to threats and ensure their networks and resources are protected.

ACTION CHECKLIST

- Maintain focus on the economic motivations driving attacks when creating an effective attack prevention plan.
- Adopt tailored defenses to deal with the spectrum of high-volume, low-value attacks vs. more targeted and time-consuming, high return attacks.
- Prioritize attack prevention measures that make it more costly to attack your site, compelling threat actors to look elsewhere.
- Deploy highly targeted friction on suspicious traffic to frustrate attackers, without harming good user throughput.



03

UNDERSTANDING THE LATEST ATTACK TRENDS

THE EVOLVING LANDSCAPE

As businesses have moved to virtual platforms, consumer behavior has been fundamentally altered. With individuals spending more time online than ever before, cybercriminals have developed new methods to target them. Here are 4 key insights on the evolving attack trends in a world of increasing digitalization:

1 With banking services now being available online, attackers have found ways to exploit security features and account confirmation processes. **Chargebacks and friendly fraud** attempts have skyrocketed since 2022.

2 New attack vectors opened as the demand in online shopping went through the roof, causing a spike in **price gouging and non-delivery scams**. Attackers will post an item for sale they do not plan to deliver or hike up the price for stolen, high-demand items. If fraud teams decline the wrong transaction, they prevent customers from receiving their goods.

3 Alongside the increasing popularity of online shopping comes the acceleration of digital payments. Financial services are seeing a rise in **card-not-present fraud** as the massive increase in digital payments becomes a lucrative target for fraudsters.

4 As more business is conducted online, more consumers are creating digital accounts. This has launched an opportunity for fraudsters to create **fake accounts** to spread in-platform and **phishing scams** by posing as the associated brand.

BUSINESS PREPAREDNESS

To successfully defend against attacks, businesses need to understand the unique ways fraudsters can target a particular industry. Attack types, goals, and methods can vary, so it is worth understanding the current attack trends in your industry and how they may impact your business. It is also helpful to understand how your organization fits into the larger attack ecosystem, so you can anticipate and prepare for potential threats.

INDUSTRY	TARGET
ECOMMERCE / RETAIL / TRAVEL Payment fraud, loyalty points, inventory hoarding, account takeover, scraping	Compromised consumer data puts retailers' customer accounts at risk of credential stuffing, ATO attacks, loyalty point theft, payment credential theft, and other personal info theft. With businesses increasingly hosted online, account security is now considered mandatory.
ONLINE GAMBLING / IGAMING Digital currency, in-game items, valuable accounts, bonus abuse	Gaming companies often struggle to detect fraud amid spiking traffic due to the massive rise in new users, allowing fraudsters to create bot accounts at scale for bonus abuse or to manipulate in-game economies.
FINTECH / BANKING / FINANCE Bank account information, payments, data	Compromised financial accounts enable attackers to drain funds or commit fraud, increasing pressure on fintechs and challenger banks to provide robust authentication without disrupting the good user experience.
TELCO / TELECOM Phishing scams, malware, DDoS attacks, account hijacking, ransomware	Attacks here are designed to disrupt operations, steal data, skew communications, and cause financial losses. As a result, telcos and telecom businesses must protect themselves from these threats, such as implementing security measures, educating their staff, and investing in a secure infrastructure, staying vigilant and continuously monitoring their network, applications, and systems.
TECHNOLOGY PLATFORMS Info scraping, spam/abuse, bonus abuse	Criminals often exploit these platforms in a variety of techniques, such as creating large amounts of fake accounts to acquire free server time on software development sites, and launching tailored ATO attacks on corporate networks to acquire confidential information or to extort money. Some attacks are not even driven by financial gain, but instead, simply intended to disturb the good user experience.

SPOTLIGHT ON ACCOUNT TAKEOVER ATTACKS

Account takeovers (ATOs) can be extremely difficult to detect and respond to, as they often involve a malicious actor taking over an existing user account or creating a new one with stolen credentials. In fact, the threat intelligence community calculates a 65% rise in the number of compromised credentials available on the dark web since 2020. This reality allows attackers to gain access to sensitive information or bypass security controls.

Businesses today should consider leveraging security analytics and threat intelligence to detect and respond to potential ATO attacks. By taking a proactive approach to ATO security, businesses can reduce their risk of experiencing a costly attack or breach.

How an attacker launches an ATO in three steps:

1. Find an open port on the target's network or system, typically by using a port scanner or other methods.
2. Send a large number of requests to the port, usually through a botnet attack or distributed denial of service (DDoS) attack. The requests flood the target's system and exhaust its resources, typically its bandwidth or processor speed.
3. Gain access to the system by exploiting the vulnerabilities of the system or application. This could be done by using specific commands, such as SQL injection or cross-site scripting, to access the target's data or system.

ACTION CHECKLIST

- Invest in strong network security and IAM to stem the leak of identity information and credentials.
- Avoid free solutions which are bypassed by bots and ensure all web forms are protected from automated credential testing.
- Monitor login attempts to digital accounts in real-time, classifying traffic into legitimate users, suspected bot, and human-driven attack attempts.
- Use secondary screening to test high-risk traffic with authentication steps designed specifically for that threat model.

[1]*https://www.spiceworks.com/it-security/identity-access-management/news/billions-of-stolen-passwords-found-on-internet/*

04

FOCUS ON STRATEGIC ATTACK PROTECTION

THE EVOLVING LANDSCAPE

Proper attack prevention is an important factor for businesses of all sizes and industries. While it is often seen as a cost center, preventing cybercrime is a key driver of profitability and an essential part of maintaining a strong brand image. With the right strategies in place, businesses can use attack prevention to not only protect their assets, but to also increase their revenue and bottom line.

By implementing the right measures to detect and deter attack, businesses can reduce their losses, protect their customers, and increase their profits. Taking steps to secure customer data can also help to build customer trust and loyalty, which further contributes to business success.

BUSINESS PREPAREDNESS

Businesses are continually challenged with balancing growth and risk while meeting the demands of cybersecurity. With customer onboarding experiences now becoming a key factor in customer satisfaction, it is more essential than ever to ensure that attackers don't have equal access. To achieve successful growth, smart risk management, and robust fraud protection, security teams must work collaboratively with product, marketing and strategy teams.

Organizations must create an environment where teams are encouraged to share ideas, discuss strategies and coordinate efforts to ensure a secure customer onboarding process that meets all customer needs. This collaboration should include the development of measures to detect and respond to any suspicious activity and the implementation of solutions that provide ongoing protection.

Additionally, businesses should take steps to educate their employees on cybersecurity best practices and create an environment of transparency and trust so that customers can feel secure in the services they are receiving.

SUSTAINING GROWTH IN 2023

- **Know your customer:** An in-depth understanding of individual customers provides a powerful basis for identity verification.
- **Bring the benefits of bricks and mortar online:** A hybrid “digital backed by people” approach provides customers with a streamlined, efficient service supported by real humans when necessary.
- **Communicate with consumers:** Provide multiple options including phone, video messaging, and online chat to best meet the needs of a diverse customer base.
- **Refine your product:** Competition is stiffer than ever, with businesses of all sizes scaling-up and benefiting from innovations like AI. The product must be excellent, user-friendly, relevant to customers, and good for business.
- **Work smarter:** Make it easy for customers to get the services they need in-house by offering relevant partner products to help streamline operations.
- **Prioritize efficiency for consumers and the business:** This doesn't just drive down costs, but should be tailored to create user-friendly products that meet individual needs.
- **Invest in attack prevention:** A proactive, rather than reactive, approach to security that integrates fraud prevention into all parts of the customer experience will not only safeguard profit and reputation, but also provide cost savings and improved return on investment.

ACTION CHECKLIST

1 PROPERLY QUANTIFY THE ROI

Fraud and security departments must demonstrate how efficiently preventing attacks boosts revenue, e.g. what is the cost savings from blocking a major bot attack?

2 EMBED ATTACK PREVENTION INTO DIGITAL

The pandemic accelerated the much-needed digital transformation of security programs. Large teams are no longer required to be on-site, servers are monitored, and even power switches turned on and off remotely.

3 STEM THE RISING TIDE

With bad actors constantly recruiting and scaling up, businesses must realize the importance of investing in robust fraud and security departments.

4 POSITION ATTACK PREVENTION AS SALES DRIVER

Strong fraud and security protocols also support marketing and sales functions, allowing these departments to demonstrate that safe user experience leads to happier customers while enabling new acquisitions.

5 MOVE THE TARGET ELSEWHERE

Cybercriminals regularly share information and details about sites with lax security controls.

05

DELIVER EXCEPTIONAL UX FOR DIGITAL CUSTOMER BASE

THE EVOLVING LANDSCAPE

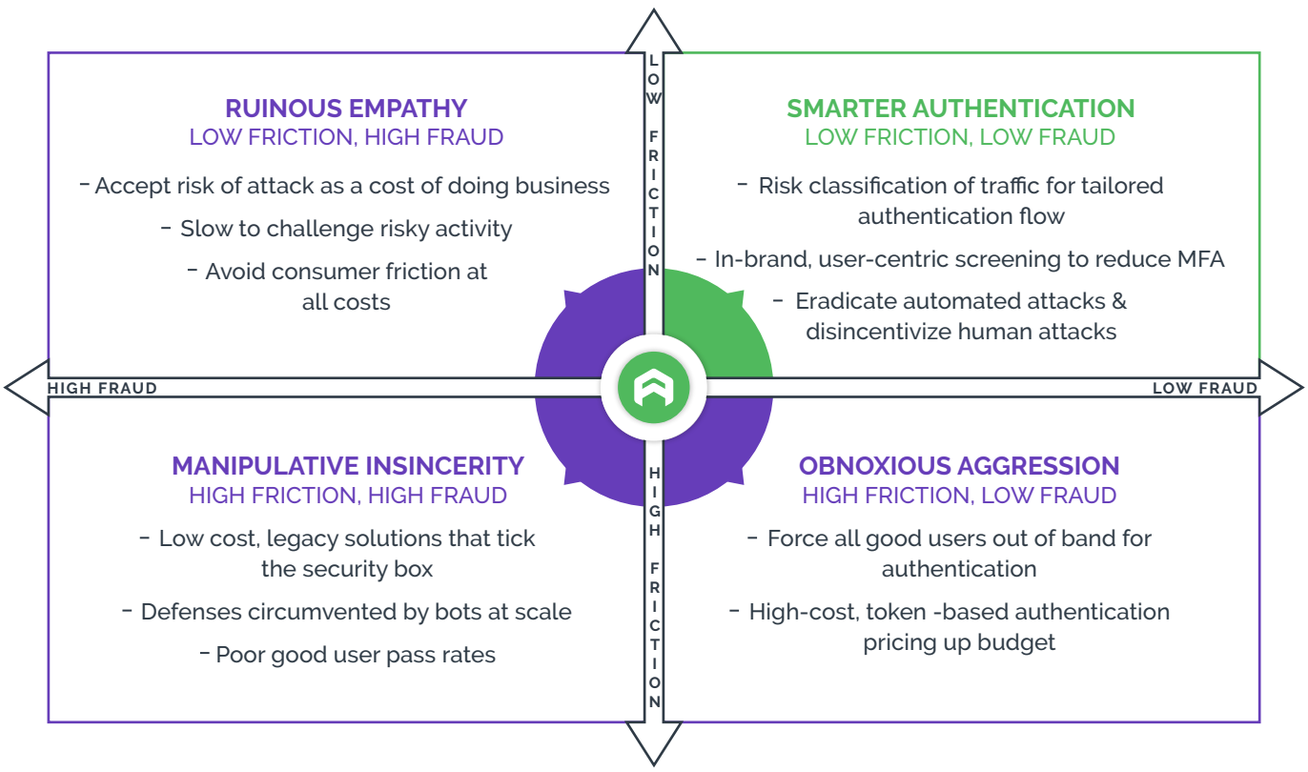
Given the extreme variability in digital traffic levels and the intensity and frequency of fraud attacks in 2022, it's highly probable that this pattern of irregular change will remain. Many companies were taken off guard after the broad digitization caused a rise in fraud, and had trouble managing this new reality. It really brought home the point that fraud and security teams will never be able to get careless, and must always be ready. Digital traffic will only go on to reach higher levels and remain at heightened amounts—it's been said that once humans develop habits, it's impossible to make them go away.

BUSINESS PREPAREDNESS

Businesses are in a difficult situation as they try to balance rising cyberattack levels with customers' expectations for fast, secure digital transactions. Consumers want to feel confident that their data is secure, but they don't want their experience to be impeded by long delays or complicated authentication processes.

As a result, some organizations have resorted to too much security, which results in good customers being forced to authenticate separately, resulting in a costly loss of business. On the other hand, some businesses have been too lenient with security, leading to fraud losses and a decrease in customer trust. The solution lies in a balance between risk assessment and increased authentication.

Business teams need to identify and interdict high-risk traffic with user-centric challenges that don't disrupt the user experience. By properly assessing risk with targeted friction, businesses can deter cybercrime without hindering legitimate customers. Friction can be an effective tool in maintaining security, building customer trust and protecting a company's reputation.



ACTION CHECKLIST

- Identify and replace any cheap or legacy security technology that fails to keep UX at the front and center.
- Deploy different levels of screening based on the risk profile, ranging from invisible risk assessments, in-session user challenges, to out of band authentication when absolutely necessary.
- Invest in a continuously learning platform that will learn from past assessments to make smarter decisions about who to challenge in the long run.
- Utilize machine learning to turbo-charge identification of emerging attack patterns while reducing customer intervention rates, to improve the overall user experience.

CONCLUSION

This playbook is intended to provide an understanding of the current and emerging cyber threats and the strategies and best practices that organizations can use to protect their systems, networks, and data. By following the guidance outlined in this playbook, organizations can develop a comprehensive cybersecurity strategy to protect their assets and valuable data. With the right combination of people, processes, and technology, organizations can dramatically reduce the risk of a successful cyberattack and protect themselves from the ever-evolving threats of the digital age. As cyber threats continue to evolve, it is essential for organizations to keep up with the latest security trends to stay ahead of the game.

Arkose Labs

The mission of Arkose Labs is to create an online environment where all consumers are protected from online spam and abuse. Recognized by G2 as 2023 Leader in Bot Detection and Mitigation, with the highest score in customer satisfaction and largest market presence four quarters running, Arkose Labs offers the world's first $1M credential stuffing and SMS toll fraud warranties. Its AI-powered platform combines powerful risk assessments with dynamic attack response to undermine the strategy of attack, all the while improving good user throughput. Headquartered in San Mateo, CA with offices in London, Costa Rica, and Brisbane, Australia, Arkose Labs protects enterprises from cybercrime and abuse.

Sales:

(800) 604-3319

Mail:

support@arkoselabs.com

Address:

USA • 2 W 5th Ave, Fl 3, San Mateo, CA. 94402
Australia • 315 Brunswick St, Fl 2, Brisbane, QLD. 4006
UK • 167-169 Great Portland Street, 5th Floor, London, W1W 5PF

Schedule Demo