Arkose Labs

EBOOK

THE CISO'S GUIDE TO THE ROI OF CYBERSECURITY

5 Ways to Articulate the Value of Your Cybersecurity Strategy

INTRODUCTION

The job of a Chief Information Security Officer (CISO) sometimes feels like a zero-sum game. From ensuring the health and security of an enterprise's network and systems to advocating for more resources and navigating heavily matrixed, global structures, there are a multitude of responsibilities on a CISO's plate. While more is expected of CISOs, shrinking resources make the job more difficult than ever. All of this comes on the heels of cyberattacks, the long-tail impacts of a global pandemic, and the rise of professional cybercrime-as-a-service (CaaS) offerings that can turn low-skill users into impactful cybercriminals.

The need to protect sensitive data keeps CISOs in the crosshairs with their boards. An FTI Consulting[1] study found that 79% of CISOs feel heightened scrutiny from senior leaders. Due to this increased scrutiny, the rise of attacks, and more, a 2022 survey[2] found that 59% of CISOs experienced stress in their role and 48% felt burned out.

We hear you, and we are here to help. One way to improve both an enterprise's cybersecurity and reduce stress and burnout amongst CISOs is to implement a bot management solution that is effective at stopping malicious bots and cost-effective as well. This move can also help CISOs achieve the desired end state of improving the overall security of their network.

However, implementing a new security solution can be expensive, and it may be necessary to justify the cost to other C-level executives or a board of directors. This has its own challenges (economy aside), especially when you consider the following[3]:

- Less than 2% of 4,621 board directors representing S&P 500 companies have held cybersecurity roles in the past 10 years
- 34% of board directors feel that their boards don't have enough expertise to govern cybersecurity

[1]FTI Consulting Survey Reveals CISOs Struggle to Effectively Articulate the Business Impact of Cyber Risks
[2]Chief information security officers say stress and burnout, not job loss as a result of a breach, are their top personal risks
[3]Ukraine War and Upcoming SEC Rules Push Boards to Sharpen Cyber Oversight

Here are five things to consider as you articulate the cost savings of an effective bot management solution:

1. The Cost of Unplanned Downtime
2. The Cost of a Customer Data Breach
3. The Cost of Reputational Damage
4. The Cost of Lost Revenue
5. Cost-Benefit Analysis

NEW: Calculate your ROI with the Arkose Labs SMS Toll Fraud Calculator. With cybercrime estimated to cost $10.5 trillion by 2025, can you afford not to?

1. THE COST OF UNPLANNED DOWNTIME

Time is money and cybercriminals armed with malicious bots are constantly looking for opportunities to steal both from organizations and individuals. Between 2014-2019, 50% of organizations had unplanned downtime incidents. Any instance of downtime, regardless of cause, is costly, with high-end estimates of more than $17,000 a minute.[4] Bot-related incidents not only have the potential to hurt a brand's hard-earned reputation, but can kill productivity. It is a time- and money-suck, that may also harm the consumer experience.

Think of it this way: Consumers have less patience than ever before. They have an expectation for quick, digital-first transactions. If your enterprise systems are down while security teams are investigating a potential attack, or if consumers experience long wait times to talk with customer service, they can go elsewhere, taking their spending power with them.

Malicious Bots & Downtime

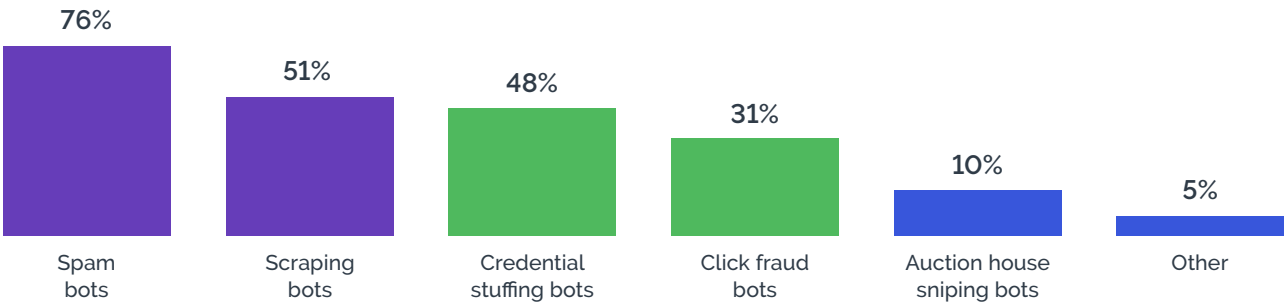
Bot attacks, and the rise of botnets, have had a massive impact on enterprises and they are only getting smarter and more widespread. In fact, 42% of internet traffic consists of bots[5]. While some of these are "good bots," many are used for malicious or fraudulent purposes. Today, bot attacks are no longer limited to spamming or small scraping attempts. Bots help attackers perform DDoS attacks and account takeover attacks, perpetrate credit card fraud, abuse APIs, and more.

More than ever, attackers use bots, and many of them are helped by AI. These malicious bots can have an outsize impact, sometimes even making headlines. In a recent example, bots seemed to play a large role in making it difficult for fans attempting to purchase Taylor Swift concert tickets[6].

[4]Cybersecurity and the Cost of Unplanned Downtime
[5]42% of Internet Traffic is from Bots – What is Your Cybersecurity Gameplan?
[6]Ticketmaster Blames Bots in Taylor Swift 'Eras' Tour Debacle

Making matters more difficult is the rise of cybercrime-as-a-service (CaaS) platforms. Would-be cybercriminals now can purchase advanced "solutions" online from criminal vendors. A user can purchase bots to run inventory scraping in which they buy a product, like concert tickets or sneakers, and sell them for a profit. Many criminal CaaS organizations provide high levels of customer service and even include "how-to" guides. This additional layer of criminal professionalism is placing more strain on enterprises than ever before.

These CaaS offerings effectively lower the barrier to entry for cybercriminals, growing the population of attackers and placing sophisticated cyber threat capabilities in the hands of users who would not have the wherewithal to conduct them otherwise. Bot attacks are as numerous as they are varied, but the common denominator is that they have negative impacts on an enterprise's bottom line. An Arkose Labs study[7] consisting of responses from 100 technology executives who experienced bot attacks found the following types of bad bots most impacted an enterprise's revenue:



It is increasingly difficult for businesses to detect these attacks in real time. Nearly three-quarters of respondents in the survey said that real-time detection of bot attacks was either extremely or somewhat difficult. This means that for some enterprises, once an attack is discovered, it may already be too late to mitigate the damage. While capital is often an enterprise's most important asset, so is time.

A successful bot attack means downtime for an impacted enterprise.

This downtime is often the hidden cost associated with any successful cyberattack, and detecting and recovering from a bot attack can take significant investment in time, manpower, and capital to get back on track. By implementing a modern bot management solution, you can reduce the frequency and impact of bot attacks, leading to less downtime and a more productive workforce. This can increase productivity, and prevent lost revenue and the loss of hard-earned brand equity.

2. THE COST OF A CUSTOMER DATA BREACH

A bot attack can result in a data breach that exposes sensitive customer data. This can lead to costly regulatory fines and damage to a company's reputation. While inventory scraping often gets the headlines when it comes to bot attacks, it is important to note that cybercriminals are always on the prowl for ways to make a quick buck or gain information that can enable future attacks. This is where customer data comes in.

[7]Modernizing Bot Attack Prevention

Customer data is a valuable asset, which is why it is increasingly regulated. Cybercriminals use bots to automate many of the actions needed to steal customer data while lurking in user login and registration flows, and they use that data for a variety of purposes. Cybercriminals sell user information, like usernames and passwords, on the dark web for easy money, and leverage it for account takeover attacks.

For CISOs, it can often feel like a ceaseless game of Whac-A-Mole. The average cost of a data breach has increased from $3.86 million to $4.24 million in 2021[8], and remote work adds to the cost.

> The average cost of a data breach is more than $1 million higher in breaches where remote work is a factor.

Data Protection Laws & Regulations

Whether it is the European Union's General Data Protection Regulation (GDPR), the California Privacy Rights Act (CPRA), or other data privacy laws in the United States, there is an array of laws and regulations with which to comply.

The alternative is expensive and potentially disastrous. Organizations face stiff penalties and fines when they mismanage consumer data. For instance, GDPR fines[9] for global enterprises can amount to 2%-4% of an enterprise's annual revenue, depending on the severity of the infringement. This can translate into approximately $10 to $20 million in fines, depending on the enterprise's revenue.

Additionally, some bot-management tools that authenticate user traffic, like reCAPTCHA, are not GDPR-compliant. Google's reCAPTCHA does not provide the requisite notice or consent to users, which goes against the letter of the law when it comes to GDPR.

> With the reputational cost of the data breach, the cost of fixing it, and any regulatory fines, the real cost of a data breach could be too high for many businesses to handle.

A bot mitigation solution can help prevent data breaches and protect customers' data, potentially saving an organization from costly fines and reputational damage, which this eBook examines further in the next chapter.

3. THE COST OF REPUTATIONAL DAMAGE

A successful bot attack can also hurt a company's reputation if customers don't believe it can keep their data safe. Cybercriminals do whatever they can to make a profit at the expense of a business and its customers, and if customers are worried about their personal data, they may take their business elsewhere.

[8]Cost of a Data Breach Report 2021
[9]What are the GDPR Fines?

C-level executives should understand the potentially disastrous reputational impact of bot attacks. An Arkose Labs study[10] found the following impacts of bot attacks in order of significance:

There are numerous ways in which cybercriminals can use bots to negatively impact an enterprise's reputation, and much of it relates to the customer experience. For instance, fraudsters use stolen data to write fake company reviews or downvote products that are listed in online marketplaces like Amazon. They steal an enterprise's web content or business data, like pricing details, and provide it to competitors. Both of these instances can, and will, negatively impact both an enterprise's brand as well as its viability on the market.

Enterprises are not spared when it comes to bot attacks that target inventory. Cybercriminals are on the hunt from shoes to video game platforms and everything in between, and this hurts the customer's perception of an organization. When consumers visit a website to make a purchase, they expect a frictionless experience. If inventory is denied and they can't make a purchase, or they can only buy an item on secondary markets at higher prices, that experience negatively impacts an enterprise and its brand.

Account takeover attacks (ATOs), which remain one of the most important issues in fraud prevention, are gaining in popularity amongst cybercriminals. ATOs occur when fraudsters gain access to legitimate user accounts.

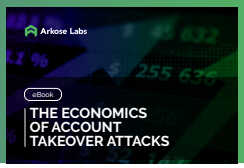
> Once a cybercriminal gains control of a user's account, they can use the account for many fraudulent purposes or follow-on attacks like money laundering, opening fraudulent lines of credit, or money muling. All of this can have a particularly insidious impact on an enterprise's reputation.

One of the major reasons for this is that it can be difficult for enterprises to gain visibility into the complete extent of the damage as a result of a successful ATO attack. ATOs negatively impact the consumer experience, resulting in the erosion of trust between an enterprise and its customers, and increasing the potential for customer churn. This can undermine an enterprise's long-term efforts of building, and maintaining, a brand as well as acquiring and retaining its consumers.

[10]Modernizing Bot Attack Prevention

All of this adds up quickly. Arkose Labs' research[11] found that companies with more than 10,000 employees reported costs exceeding $1 million, while 10% of companies had losses between $500,000 and $1 million. The true costs are actually higher, as these costs don't include the negative impacts due to downtime, operational costs, recovery efforts, and reimbursements to customers for loss of funds due to an ATO attack.

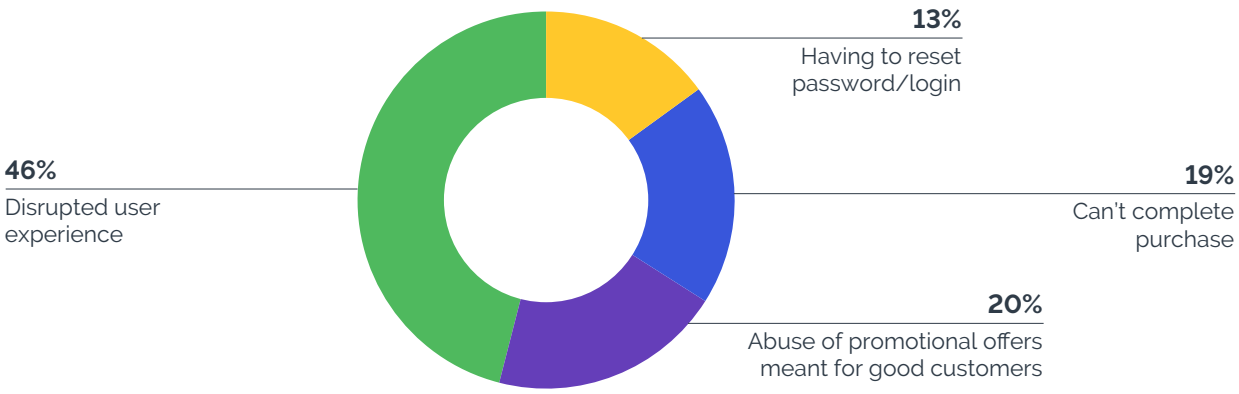
Get more details on the true cost of an ATO in the eBook:
The Economics of Account Takeover Attacks



By implementing a bot mitigation solution, one that proactively stops attacks like ATOs at the front door, CISOs can protect their organization's reputation and maintain customer trust, potentially leading to increased customer retention and revenue.

4. THE COST OF LOST REVENUE

The reasons for evaluating a cybersecurity solution include reduced downtime, protection of customer data, avoiding reputational damage, or all of the above, it all comes down to protecting your enterprise against lost revenue. Arkose Labs' research shows that bot attacks had the following negative impacts:



Nearly half of respondents stated that their end users' experience had been disrupted as a result of an attack. Even seemingly minor setbacks, like having to reset a password, for instance, can have an impact on an enterprise's bottom line. To that end, there may not be a better investment than a bot management solution that stops fraudsters in their tracks. The reason is that bot attacks regularly cost enterprises lost revenue, as customers may be unable to access your systems and inventory or may decide to take their business elsewhere due to a lack of trust in your security measures, especially in instances of ATOs.

[11]Account Takeover Survey: Top 7 Findings on the Impact of ATO

Case Study: International Revenue Share Fraud (IRSF)

A well-known social media platform[12] implemented one-time passwords (OTPs) sent to a user's phone or email upon registration as a security measure to verify a user's identity and protect their account (when returning to login) from unauthorized access; however, attackers flocked to the platform to abuse the OTPs at registration, which is known as international revenue share fraud (IRSF). Cybercriminals make money off of this scheme by colluding with high-cost telecommunications companies and use automated bots to make accounts with phone numbers where they profit on every SMS message sent to numbers they own. These attacks can result in millions of dollars in fraudulent SMS bills for the enterprise.

The social media company's SMS bill was dramatically reduced after deploying Arkose Labs on their website and apps to detect bots carrying out IRSF, mitigate that malicious activity and protect the company's revenue.

The platform saved $3 million per month in fraudulent SMS charges. By putting Arkose Labs in front of the SMS flow, the platform saw an immediate reduction in infrastructure costs by removing high volumes of malicious bot traffic.

When it comes to thwarting the multitude of threats facing an enterprise, having a solution that counteracts much of an attacker's automated bots is key. By implementing a bot mitigation solution, you can prevent these attacks and protect your organization's revenue streams.

Enterprises can insert Arkose Labs at any touchpoint which is protected by one-time passwords, such as the login flow or new account registration, in order to detect fraudulent traffic. Furthermore, due to Arkose Labs' unique in-session authentication that combines real-time risk classification with interactive MatchKey challenges, organizations can rely less on multifactor authentication methods.

Additionally, these challenges ensure that good users are never blocked, which enables genuine, revenue-generating traffic.

5. COST-BENEFIT ANALYSIS

One way to clearly articulate the cost savings of a bot management solution is by conducting a cost-benefit analysis. This involves weighing the costs of implementing the solution against the potential costs of not implementing it. For example, a CISO could compare the potential costs of lost revenue, reputation damage, and regulatory fines due to a bot attack versus the cost of implementing a bot management solution. This can help other C-level executives or directors understand the potential ROI.

[12]Social Media Platform Saves Millions in SMS Fraud with Arkose Labs

Use Arkose Labs SMS Toll Fraud Calculator to quantify your ROI with easy-to-understand dollars and cents savings!

A cost-benefit analysis of a cybersecurity solution could include the following:

1. Implementation costs: including hardware, software, and personnel expenses.
2. Maintenance costs: such as upgrades, patches, and support fees.
3. Cost savings: the reduction in risk of data breaches and financial losses.
4. Revenue potential: including increased customer trust and reputation.
5. The cost of inaction: including potential penalties, lawsuits, and business loss due to a lack of security measures.

According to Cybersecurity Ventures, cybercrime has a global annual cost of $8 trillion, and investing in cybersecurity measures can result in significant ROI. Not only does it reduce the risk of a damaging attack, but it can also help to reduce the amount of time and resources needed to respond to and recover from a security breach.

Case Study: SMS Toll Fraud

One of the world's most popular video game developers[14] was losing $1 million per month due to International Revenue Share Fraud (IRSF), which is also referred to as SMS Toll Fraud. Cybercriminals targeted the developer's registration process in which a weakness in the SMS validation process enabled the attacker to profit from resulting SMS toll charges.

To address this problem, the developer implemented Arkose Labs' solution at all touchpoints that were protected by one-time passwords (OTPs) in its account registration process to detect fraudulent traffic. As a result, the video game developer saw a significant reduction in fraudulent SMS charges, saving $1 million per month.

The Arkose Lab solution also created additional positive downstream benefits, including reduced support time managing compromised accounts, decreased fraud case management, lower disruption rates for new customers, and reduced infrastructure costs. All of this came with a more secure and frictionless user experience.

[13]Cybercrime to Cost the World 8 Trillion Annually in 2023
[14]Popular Video Game Developer Saves $1 Million per Month Working with Arkose Labs

Do you want to know how your own enterprise can experience savings in the face of IRSF? Our newest tool, the Arkose Labs SMS Toll Fraud Calculator, provides enterprises a way to calculate and articulate their contributions to the overarching priorities of the enterprise, including the percentage decrease of cyberattacks and the hard dollar amount of investment return. Check out our ROI calculator today and discover how much cost savings your enterprise can find this year!

How Can Arkose Labs Help?

Financial incentives fuel all fraud. Arkose Labs delivers long-term bot management and account security by undermining the economic drivers behind attacks. We help enterprise customers defend the most targeted user touchpoints by uncovering hidden attack signals and sabotaging attackers' ROI without sacrificing good user throughput.

Arkose Labs' unique detection and mitigation platform analyzes data from user sessions to determine the context, behavior, and past reputation of every request. We classify traffic based on its risk profile and present suspicious traffic with enforcement challenges to differentiate between true users and fraudsters.

An effective and modern bot management solution can help by reducing downtime, protecting customer data, avoiding reputation damage, and protecting against lost revenue. When it comes time to conduct a cost-benefit analysis, examining the costs of being negatively impacted by cyberattacks should be balanced with the benefits of an effective solution.

While investing in a solution to combat the multitude of cyber threats an enterprise faces costs money, the right solution will not only protect against these negative impacts, but help to maximize an enterprise's ROI as well. As a CISO, you must clearly articulate these cost savings to your board of directors to ensure they understand the value of implementing this solution.

Want more information on how Arkose Labs can partner with you to quickly and effectively remediate automated and human-driven fraud? Book a demo with us today!

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.

support@arkoselabs.com

Address:

USA • 250 Montgomery St, Fl 10, San Francisco, CA. 94104

Australia • 315 Brunswick St, Fl 2, Brisbane, QLD. 4006

United Kingdom • 167-169 Great Portland Street, 5th Floor, London, W1W 5PF

Schedule Demo