3rd-party code playbook

The AdMonsters
Third-Party Code Playbook

November 2013

01 about

admonsters

Founded in 1999, AdMonsters is the global leader in providing strategic insight on the future of digital media and advertising technology through its conferences, website, research and consulting services. AdMonsters focus is on media operations, monetization, technology, strategy, platforms and trends. Its conferences and website are the meeting place for this dynamic and expanding community to connect, gain insight, develop best practices and exchange thought leadership. AdMonsters conferences include AdMonsters Publisher Forum, OPS, OPS Markets, OPS Mobile, OPS TV and AdMonsters Screens. In the early days of online media, the community was comprised largely of operations professionals at online publishers and advertising technology providers. Today's expanding ecosystem now includes publishers and content creators, agencies, SSPs, DMPs, DSPs, RTB and service providers, technology and platform developers, advertising networks, brands and investors.

For more info:
See admonsters.com
Follow us on Twitter: @AdMonsters
Facebook: facebook.com/admonsters

Sponsorship contact:
Dan Halioua, VP, Sales
dhalioua@admonsters.com
tel: +1 917-428-8085

Media contact:
Stacy O'Connell, VP, Marketing
stacyo@admonsters.com
tel: +1 415 480-4114

TMT The Media Trust

The Media Trust provides automation and monitoring services for online and mobile ad ops, site ops, and site security organizations across the entire advertising technology ecosystem. Our ad creative and website quality assurance, data transparency, vendor certification, and malware/malvertising monitoring services are used by hundreds of clients across 65 countries including 40 of Comscore's Top 50 Media Metrix Multi-Platform properties, hundreds of ad networks, and the predominance of SSPs and exchanges.The Media Trust combines these best in class services into the industry's only holistic creative and website quality automation service.

Please visit themediatrust.com to learn more.

02 introduction

At some point in the history of the Internet, someone placed code on their website that called an external third party to help it deliver content or provide functionality for that website. A digital miracle? Well, perhaps that's taking it too far, but still imagine for a second how liberating that must have felt for web developers who no longer had to build everything themselves but could share code back and forth.

Third-party code took the Internet from a place of hobbyists and scientists to its current state as an integral part of our culture. Today the development of any website is an amalgamation of code from a variety sources.

However, the invention and proliferation of third-party code also opened a Pandora's box as website owners were no longer 100% in control of their sites. A host of issues can arise because of third-party code, including failure of the site to load, malware, data leakage and more.

For site owners, these are acceptable risks considering the potential rewards of third-party code – especially sites where the primary revenue source is advertising. All but a small fraction of digital advertising requires third-party code to deliver, track and ultimately bill on the display of advertising.

Third-party code may giveth revenue, but it can also taketh away: failure to mitigate against the risks can lead to loss of revenue, depletion of audience and even serious legal issues. The dangers may never be completely removed, but an active management strategy enables website owners to protect themselves while growing their business, and possibly help generate further revenue.

03 what's a playbook?

A playbook is an extension of what the AdMonsters community has been doing at our conferences for over 14 years. A playbook solidifies what has made our events "must attend" for many digital strategists. By bringing people together to share learnings and best practices in a focused way, people can create a plan and avoid hours—if not days—of doing research on their own.

The AdMonsters playbook concept takes existing AdMonsters content (from conferences and AdMonsters.com) and, with the help of the AdMonsters community, "crowd sources" a document that outlines best practices on a particular topic. Our belief is that this will allow for a free exchange of ideas with the benefit of curation for accuracy.

The point of this playbook is to instill readers with a knowledge of the risks associated with the use of third-party code, and the serious consequences of a failure to mitigate. It also provides the policy and process strategies for managing these risks effectively, efficiently and across an organization.

This document does not get into specifics around individual solution providers intentionally. Monitoring solution providers were excluded from the research of this document, as it's our belief that this playbook should be written by technology end users for technology end users.

Great effort has gone into writing the playbook in a fashion that applies to as many publishers as possible without becoming too general. In a technology-driven industry like digital advertising, information quickly becomes obsolete. The intention is that, based on the feedback of the AdMonsters community, the next version of this playbook will start to take shape and, with additional contributors, grow in both depth and breadth. Publication of future versions will be scheduled based upon the needs of the community.

04 why active management?

Simply trusting third parties to deliver on their promises is an insufficient way to mitigate the risks associated with third-party code. By definition the code is managed by a different party than the website, so its behavior may change without notice. Code can even simply disappear. Here are some possible cases in which third-party code could wreak havoc on a website.

- A provider might cease to exist overnight, leaving a call to a server that no longer responds and delaying delivery of the web page.
- A third-party could change its policies about what data they collect and begin profiting off a site's audience without the knowledge of the website owner.
- A third-party could change the partners it works with, potentially exposing website visitors to malware, data leakage, latency and more.

For many companies, the management of third-party code is siloed between editorial, most likely relying on an IT department to monitor code, and ad operations, managing code served through the ad server. That division of focus isn't necessarily wrong, but ultimately the policies, partners and processes of anything related to third parties should be company-wide. Active management of third-party code is a cross-departmental problem to solve.

Code vs. Tag

In this playbook, we refer to "third-party code" instead of "third-party tag," which is the common term used within digital advertising to refer to the code that delivers the creative. While some of our recommendations are focused on third-party tags and digital advertising specifically, it's important to think beyond ad calls to other third-party-served code on a page. For example, a widget placed on a site by the editorial team via third party code may not have a single advertising component, but has the same potential vulnerabilities as third party tags.

05 areas of risk

Malvertising.

The fight against malvertising (malware delivered through advertising) is a battle that few know we are locked in. Malvertising most often is not the work of an angry teenager striking out at the world, but an organization that profits from weaknesses in the digital media ecosystem. It's a big business and relies on people not paying attention to the code they place on their sites through ad placements or other tags.

The infected site is the one who ultimately gets blamed, resulting in a loss of users, revenue and brand equity. The costs of reducing the likelihood of malvertising being served certainly outweigh the consequences of it getting through and launching a publicity nightmare.

Latency.

Amazon has found that every 100 milliseconds of latency equals a 1% drop in sales. Google has found that an extra 500 milliseconds in search page generation time makes traffic drop by 20%. Website owners need to provide content as quickly as possible and work with third parties to reduce latency. Like malvertising, it's the website owner that is left holding the bag.

The problem isn't simply how fast an ad server returns an ad, but all the third and fourth parties involved in setting cookies or delivering content through that ad server. Sites are only as fast as the weakest partner in the chain of external parties called on each page.

Creative QA.

The images and text (or "creative") served through third party code can affect revenue. People judge the quality of a website on what they see and will continue to interact with that website based on how secure of an environment they feel it is. Especially for sites that generate revenue through advertising or e-commerce, the appearance of inappropriate advertising reflects on the quality of the website, and therefore will impact potential revenue.

Low-quality advertising is also a signal to users to how the site is designed, helping them decipher the content they want versus annoying – and potentially harmful – ads. Running poorly designed ads also aids "banner blindness," increasing the likelihood that users will ignore more relevant advertising when served.

Part of the creative QA process is preventing advertising from competitors. Before programmatic buying, this was a simple process. With programmatic buying, advertising from competitive sites can slip through the cracks unless there is continual monitoring.

Data.

It's hard to quantify opportunities lost, especially when it's not even being detected. While a third-party partner may say that they aren't setting cookies and tracking your users beyond the walls of your site, it does happen. You can't simply take them at their word.

05 areas of risk

More likely, however, your partner is working with other companies that may use data collected on your site for their own purposes. Chains of companies working together passing your user data back and forth are unlikely to have your best interests in mind. In fact, they may be using that data to compete against you. Falling CPMs can be partially attributed to publishers helping drive prices down by giving away their data (knowingly and unknowingly) to the competition.

Not All Publishers are Actively Managing Third Party Code

AdMonsters and Acceleration have teamed up to produce the Publisher Maturity Index (PMI) which allows publishers to measure their best practices against other publishers. In the initial findings:

84% are not monitoring 3rd party data collection

While the other initial finding indicate that more and more publishers are developing programmatic strategies, the lack of monitoring of what data is collected is alarming. Without monitoring, a publisher cannot know if their terms and conditions are being followed and the value of the media cannot be properly negotiated. Not monitoring is akin to a retail store failing to install security cameras and leaving the front door open.

42% have no dedicated QA process

In previous AdMonsters' surveys, we found that almost all ad operations leaders consider a creative QA process to be a top priority for their department, but not all could dedicate resources to that process. The result is an essential function that is only properly addressed as time permits based on other pressing responsibilities. As more creatives come from more sources through programmatic channels, publishers without a dedicated QA process will have less control of what appears on their site.

63% have no formal vendor certification process

Developing a formal vendor certification process is a time-consuming, multi-departmental headache for Ad Operations. However, our analysis show that 52% of respondents who ranked their ad tech ROI at 3 or lower do not have a vendor certification process. Conversely, 69% that have a vendor certification process ranked their ad tech ROI at 4 or higher. We feel there is a correlation between those that properly vet their tech partners and their overall satisfaction with those partners.

For more information on the **Publisher Maturity Index.**

06 addressing these concerns

These risks can be mitigated and for a large part eliminated. The key is how determined the overall organization is to taking on these risks. This determination will define the policy which will then help determine the partners and the process required to take on this challenge.

Best Practice:

Vendor Approval Processes and Certification Programs

Part of managing third-party code is managing the third parties themselves. All publishers should have an approval process that must be completed before the third-party code can be set live on the site. Many publishers have formalized this approval process into a certification program. The terminology is not important, but the enforcement is. Any such process needs to be mandatory and give the people responsible the authority to do it properly.

Third parties will approach a publisher from a variety of sources – agency, client, the vendor itself, or even internally. All are interested in getting the code approved and on the site as quickly as possible. Publisher sales teams often fail to understand that the process of evaluating vendors and code is time-consuming. To allow sales to fast-track the approval process such that the necessary steps are not taken puts everything at risk.

The first step in this approval process is collecting the necessary information on the third party. Many publishers require the third party itself to fill in the information. The Weather Company, for example, uses an online form with required fields that must be filled out before the process can begin.

The necessary questions for this form should be aligned with the company's policies around data collection, privacy and latency. Work with the IT department to formulate questions that help determine if a third-party can scale properly if needed. Legal should be part of the process in developing the form as they will ultimately have to sign off on the third party as well. Do not neglect to ask for financial information as publishers are often the ones who don't get paid when third parties fail to pay their bills or disappear.

Once the form is completed, the evaluation of the third party should be considered a multi-departmental project and managed as one. From reviewing the form to testing code, someone will need to be responsible that all the steps are completed. These steps as well as the results should be well documented.

The form and the evaluation process will continually need to be reviewed and updated. As third parties introduce new functionalities, new issues will need to be addressed.

07

malvertising: friend to no one

It's quite simple: malicious code has no place being served on your site. Your policy should focus on prevention as well as include a plan in the event malware or malvertising is served. It is not enough to check the code once or simply trust a third party: the policy should state that every third party code should be checked and monitored for as long as the code is on the site. The code should be easily removed or disabled should a problem arise.

Malvertising does not just come through programmatic means and therefore policies must be put in place for direct sales channels. Credit and background checks of potential clients should be required before ads are trafficked, regardless of how hard the client pushes for the campaign to launch. Malvertisers prey on people willing to take shortcuts..

Often malvertising will be delivered with the creative for premium brands. Always question if the buyer could actually be a legitimate source of business for a brand. Require a phone call confirmation of the deal if it looks suspicious – malvertisers are rarely equipped to handle such scrutiny.

Malware and malvertising may be designed to appear normal on the initial evaluation but change later. It's therefore essential that third-party code be monitored for the entire time it is being delivered on the website.

Ad operations is typically tasked with checking for malvertising, but all third-party code should be monitored. Solutions and processes should be considered that can address all third-party code on the site regardless of the source.

The customer service department should be educated on company policies and be prepared to alert the proper teams if a malware report is made. In addition, customer service should have a list of proper questions to ask in helping determine the source of the malware.

An escalation plan should be developed in the event malware or malvertising is served on the site. The plan should include instructions on how to quickly narrow down the possible sources. While the source is being hunted down, all departments should be notified and kept in the loop on the severity of the problem. A communication plan to consumers should already be prepared before a problem occurs.

Part of malware prevention is not only being alert to possible attacks, but spreading the word to other publishers if you feel your site has been attacked. Get clearance from management to be active in anti-malware discussions around the ecosystem.

07

malvertising: friend to no one

Process/Checklist for Malvertising

- □ Check all contracts for suspicious behavior.
- □ Perform background checks on buyers.
- □ Scan all creatives before placement.
- □ Scan all creatives from different geographic locations and different targeting parameters.
- □ Monitor all third-party code for changes
- □ Have an escalation plan should malware/malvertising be served on the site.

Resources

www.admonsters.com/blog/cracking-mobile-guide-mobile-malvertising
www.admonsters.com/topic/malvertising
www.anti-malvertising.com/
www.otalliance.org/resources/malvertising.html
groups.google.com/forum/#!forum/dclk-malvertising
msmvps.com/blogs/spywaresucks/default.aspx

08

latency: lack of speed kills

Publishers are always concerned about the overall speed of their site, but many have not explicitly developed policies to deal with latency from third-party sources. The result is multiple departments, acting independently, place code on the site and the buildup ends up affecting user experience. Policies should tie together service level agreements (SLAs) with third parties, review and monitoring of third-party code and overall tag management strategy.

In structuring an agreement with a third party, consider that latency costs you money. SLAs should outline the requirements of the third party and possible penalties if sufficient latency occurs.

All third parties should go through a technical certification process to determine the response time of their services and their ability to scale. This should be a key concern in dealing with small or new companies that may not be ready for the amount of calls coming their way once their code is live. It doesn't mean these companies shouldn't be considered, but that you should know the amount of risk is involved in putting their code on your pages.

Monitoring of latency is key and the responsibility should reside with either IT or ad operations – or both. The departments should work together on the policies and be in continual communication about what is going on with the 3rd parties they work with. Restrictions on who is able to put third-party code on the site should be built into the publishing process.

Policies around latency will not be effective without a tag management strategy. If third-party code is slow or fails to respond, that code should be removed or worst case delivered after the rest of the page loads.

As more consumers turn to mobile devices, understanding what third-party code will even execute in these environments will become more and more important. Third-party code may futilely attempt to set a cookie on a smartphone and only slow down site response time. Since mobile devices typically have slower connections than desktop computers, the risk of this unnecessary latency should be eliminated as much as possible.

Side Note on Load Times and File Sizes

From: **Formulating a Programmatic Buying Policy: Ad Quality and Traditional QA** by Chris Olson, The Media Trust

If you have a few minutes to adapt your policy from the traditional to a more modern and enlightened approach, drop "creative" file size and load time and move to TDS (Total Download Size) across the entire ad execution. We do not recommend spending resources tracking down individual pixels that take X milliseconds to load or creative that max out at greater than 50k.

Trying to enforce an issue around an individual pixel or ad in RTB is complicated at best. Instead, put rules around how long it takes for the creative PLUS the additional request chain activity to execute. The same goes for the overall size of the creative plus all other source code running with the ad. Give your

08

latency: lack of speed kills

partners a number that they can utilize as a goal and work with them to meet it.

Here's one way to think about it – You are a truck driver pulling up to a bridge over a vast chasm. The sign says maximum weight 10 tons. Before you left the warehouse your payload weighed in at 5 tons. You have no idea how much your truck weighs, but remember that a friend of yours said that by law the maximum that an 18 wheeler can weigh is 12,500 pounds. You're not driving an 18-wheeler but your truck is pretty big. Do you want to take the time to analyze how much the gas in the tank weighs or do you just want to make sure your overall weight isn't going to break the bridge?

Measuring load times and file sizes for individual components of an ad execution comes down to miniscule increments – you don't have the time to review every pixel execution that takes more than 10 milliseconds to load. If specific cookies or pixels are causing you issues it will become apparent over time.

That's a bad thing for the user in any context, but now that Google and Bing are moving to factor page load times into their rankings, it also degrades the publisher's traffic from search referrals. So publishers have a basic operational need to clean up their pages and manage down the overpixelation that's going on. The Media Trust helps them do that by measuring the latency impact from individual pixels, ushers, and collectors.

Process/Checklist for Site Latency

- Hold third parties responsible for latency by including SLAs within contracts
- Test latency as part of your creative QA process
- Determine acceptable site delivery speeds standards company-wide
- Create a process by which all third-party code is tested before being placed on the site
- Develop within your publishing process an easy way to remove tags that are creating latency
- Continually monitor page load

09

creative QA: judging by the cover

Reviewing creative for aesthetics and functionality can be a challenge, as outlined in The Ad Ops Pat Down: The Creative QA Process. From a policy perspective, it's important to work upfront to prevent time-consuming processes from taking over the ad operations department. This can be done by establishing creative specs that are clear, concise and understood by the sales team. While it doesn't always work, it can help reduce surprises down the line.

For direct sales, it's important to educate them on the risks of not checking every creative and approving before the campaigns go live. This will always be a tension point between sales and operations, so it's essential to get management signoff on the policy and, more specifically, sales management on what acceptable turnaround times will be. This is a function that can be outsourced to an outsourcing company or partner.

For advertising that comes through from networks or exchanges, it's important to understand what controls they provide to prevent unwanted ads from appearing on the site. Like latency issues, language addressing these issues should be incorporated into the agreement with the necessary partners.

You will need to decide whether advertising can come through these programmatic channels automatically—with rules for blocking added as needed—or if you are going to be restrictive upfront. This will come down to the company's tolerance for unwanted ads appearing at all. Being overly restrictive tends to yield lower CPMs; therefore a balance between the two extremes should be established.

In our research, many publishers assign creative QA responsibilities to all traffickers. Operationally that makes a lot of sense—not everyone can dedicate resources just to creative QA. The problem is when creative QA is considered a secondary priority or a task that can be sped through if other more time-sensitive responsibilities come along. This will ultimately result in the creative QA process failing and third-party code policies being ineffective at best.

The solution is to make the organization understand the indispensable nature of these processes and the resources required. If additional headcount is not a reality, look to partners to outsource or automate the creative QA process.

Process/Checklist for Creative QA

- Develop and maintain creative specifications documentation for sales and clients.
- Build a creative QA checklist for ad operations that must be completed before an ad is trafficked.
- Work with sales on a regular basis to maintain block lists.
- Document the decisions made in the creative QA process on why an ad was accepted or rejected. Use this documentation to make updates to the specifications.
- Track QA time per creative to establish necessary baselines of what time is needed. Policies on creative evaluation should reflect these baseline metrics. Also use this analysis to find ways to reduce the time required by automating or outsourcing part of the process.

10 data: it’s only your audience if you protect it

The usage of data in the digital advertising ecosystem is a free-for-all in more ways than one. This makes putting together a cohesive data policy as it relates to third parties exceptionally difficult. There are a few key concepts upon which to develop such a data policy, though the policies themselves will vary greatly publisher to publisher.

First and foremost, one cannot develop a data policy related to third parties without first finding out what data is being collected. The question of data collection should be part of the discussion from the very start and monitored throughout the life of that third-party code being live on the site.

Contracts aren’t enough to deter data being collected. Checking tags before they go live isn’t enough. Only continual monitoring can insure that the data may be handled as instructed. A variety of tools exist to track what cookies are being set and by whom. The key is that this monitoring be applied to not just ad tags but all third-party code.

Most publishers will be shocked at seeing how many third parties are collecting data on their websites. There will be cookies set by companies you are not even doing business with. Policies around this, however, get complicated very quickly. Unfortunately simplistic approaches (“no one can collect data”) are bound to fail or negatively affect revenue significantly. Many third parties have built revenue models around publishers simply giving them data – disallowing this collection will probably end relationships.

The answer is to come to an agreement with all third parties about what data they collect and for what purposes. The policy should be developed to make sure the value of that data is in line with the goals of those companies. Allowing Facebook, for example, to collect data from code that allows users to more easily share your content with others may drive enough traffic to justify using it. Understand that data collected is being used to create ad products for sale to your potential customers.

The policies therefore must help manage this balancing act of allowing what’s necessary and not giving too much away. Companies should routinely re-evaluate what is and is not acceptable, informed by the tracking of third-party activity.

11

education & internal buy-in for your policies

In The Ad Ops Pat Down: The Creative QA Process, we likened the role of ad operations to that of stadium security. Any security role is limited or strengthened by the support it gets to enforce the company's policies. Getting that support is the first step in creating an enforceable policy and without support, no policy really exists.

In our research, the biggest variable into how much time and effort was spent in actively managing third party code correlated to upper management's understanding of the affect the issues could have on their business. For some ad operations leaders, there is a sense of resignation that they aren't being heard and their efforts to enforce policy are futile.

The answer that emerges to this question at AdMonsters conferences time and time again is that the role of ad operations is that of educator to others in the company. Because of operations' unique role within the organization, there is a perspective the department can offer that others will not see.

Often the problem in convincing others is not speaking their language. IT will understand concerns about security. Editorial will understand impact on users. Management will understand revenue. In trying to create an enforceable policy, educate others based on what is important to their function within the company and base success on numbers they will understand.

There is little use in creating policies that don't apply to other departments. As previously mentioned, third-party code does not only come from ad products, but social media widgets and the like. A widget to help share website content with others can collect data, create latency and be susceptible to malvertising and should go through the same processes as a creative from an ad agency.

A multi-departmental approach will also bring up the issue of who should be responsible for enforcing policy. Our experience is that the IT/technology team should be looking at security as a whole and be involved in the processes to enforce policy. Ad operations, which is looking at new third party code every day, should own the ad serving portion of this. The two departments need to be aligned and working together.

12 summary

For most publishers, third-party code is a necessity for site experience and revenue practices. Therefore, mitigating the laundry list of potential risks – such as malvertising/ malware, latency, creative QA and data leakage – should be a top priority.

This playbook is designed to be a starting point in building policies and processes around third-party code. As a next step, we strongly suggest you speak to your peers to get anecdotal evidence of successes and challenges – especially when it comes to driving inter-organization cooperation. When approaching service providers for assisting in checking and monitoring third-party services, be prepared – know what your organization needs, and know you have full company support in procuring it.

The Media Trust keeps third-party code in check.

✓ **Malware/Malvertising Monitoring**
Protect your website and ad tags from malicious and potentially malicious activity.

✓ **Data Transparency**
Identify audience data security issues originating from ad tags or website code.

✓ **Creative Quality Assurance (Technical)**
Check that your technical creative policies are being met automatically.

✓ **Creative Quality Assurance (Brand);**
Ensure ad creatives are safe, protect your direct advertising partnerships and eliminate channel conflict.

✓ **Vendor Certification Program**
Certify that advertisers and content partners meet your malware, data, and technical quality requirements.

✓ **Desktop, Mobile/Device, Display, Video, Content**

The Media Trust's comprehensive, yet easy-to-use ad tag and website scanning solutions empower ad operations teams with unmatched ad and site quality management services ensuring security and transparency for our partners and clients. TMT services enable you to boost performance, save time, and ensure revenue continuity.

TMT The Media Trust
6861 Elm Street, Suite 3A, McLean, VA 22101 | clientsfirst@themediatrust.com

www.themediatrust.com