Osterman Research
WHITE PAPER

White Paper by Osterman Research
Published **September 2021**
Sponsored by **PerimeterX**

Shadow Code: The Hidden Risk to Your Website

Application Security Risk Survey 2021

Executive Summary

Osterman Research conducted a large survey to uncover the extent and impact of third-party scripts and open-source libraries that are used in web applications in organizations across industries. These scripts and libraries—often added without approval or ongoing security validation—can introduce hidden risks into the organization and make it challenging to comply with various privacy regulations. Collectively referred to as "Shadow Code," these scripts and libraries are used for tasks like ad tracking, payments, customer reviews, chatbots, tag management, social media integration, or other helper libraries that simplify common functions. The goal of this survey was to understand the hidden risks that organizations face from the unmanaged use of Shadow Code.

ABOUT THE SURVEY

This is the third annual survey conducted by Osterman Research for PerimeterX on the use of Shadow Code in web applications. The most recent survey was conducted during May and June 2021, and it follows a survey of 501 respondents in 2020 and 307 respondents in 2019. All of the survey respondents are security professionals or developers who are familiar with the way that third-party scripts are used by their organizations. In the current survey, the primary purpose for their organization's website(s) was one of the following:

- Retail and e-commerce for consumer or industrial customers
- Financial services for customers to manage accounts
- Travel and hospitality for customers to book reservations, manage their participation in loyalty programs, book airline reservations, etc.
- Media/Entertainment for customers to purchase digital media, play, meet others (e.g., via dating apps), etc.
- Gaming
- Delivery services

KEY TAKEAWAYS

Here are the key takeaways from the analysis of the 2021 survey:

- **Nearly all websites contain third-party code**
  Over 99% of respondents reported that their website uses at least one third-party script, and almost 80% said that these scripts account for 50 to 70% of a typical website.

- **Third-party code leaves organizations vulnerable to digital skimming and Magecart attacks**
  More than 50% of respondents believed there was some or lots of risk in using third-party code in their websites and applications. This code comes from supply chain partners who may themselves obtain code from their partners, lengthening the software supply chain and increasing business risk.

- **Code changes are frequent, but undetected**
  Over 50% of respondents state that the third-party scripts running on their web properties change four or more times every year. However, only 34% have the ability to detect changes or updates made on their website that could potentially lead to a security problem.

> ***Only 34% of respondents have the ability to detect changes or updates made on their website that could potentially lead to a security problem.***

- **Visibility into third party code is lacking**
  Website owners lack the visibility into third-party code to know for certain that their site is safe from cyberattack. Nearly 50% of respondents could not definitively say their website had not been subject to a cyberattack.
- **Client-side data breaches have severe consequences**
  More than half of respondents named brand damage, loss of corporate reputation, loss of future revenue and potential lawsuits as "huge" or "major" problems resulting from an attack.
- **Security professionals have an urgent need to manage third-party code risk**
  75% of respondents intend to purchase solutions to address website script vulnerabilities within the next 12 months.

ABOUT THIS SURVEY REPORT

The survey and this report were sponsored exclusively by PerimeterX. Information about the company is provided at the end of this report.

Website Threats and Consequences

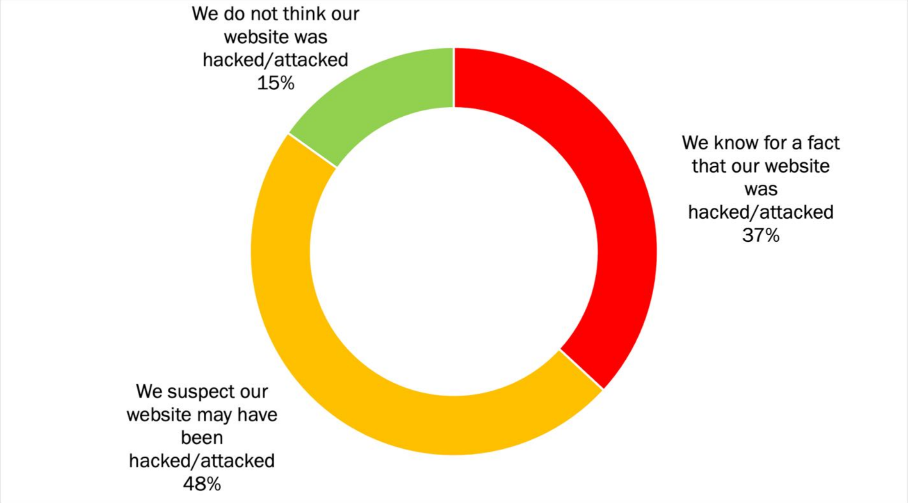
In this section, we look at the threats and consequences of cyberattacks against websites.

KNOWLEDGE OF WEBSITE CYBERATTACKS

A surprising (37%) of the respondents we surveyed knew that their website had definitely been subject to a cyberattack, while nearly one-half (48%) believed that it probably had endured such an attack. Only 15% believe their website had not been the target of a cyberattack. See Figure 1.

Website owners lack the visibility into third-party code to know for certain that their site is safe from cyberattack.

Figure 1
Knowledge of Website Cyberattacks
Percentage of respondents



Source: Osterman Research (2021)

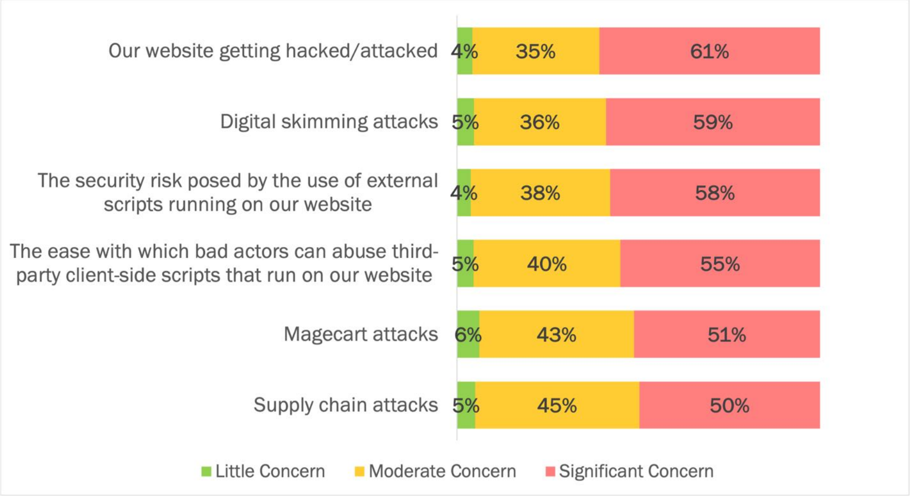
When comparing the 2021 survey data with that of 2020, we found that the proportion of those who knew for sure that their website had been attacked was virtually identical: 38% in 2020 and 37% in 2021. However, we did find some differences between the data:

- In 2020, 22% of respondents did not think their website had been attacked, compared to just 15% in 2021.
- The percentage of respondents who suspect their website may have been attacked—but lack the visibility to state definitively either way—grew from 40% in 2020 to 48% in 2021.

SIGNIFICANT CONCERN ABOUT THREATS

Experts knowledgeable about their organizations' web applications expressed a significant level of concern about seven types of threats. We found that more than three in five respondents (61%) are concerned about their website getting hacked or otherwise attacked, and nearly this many (59%) are this concerned about digital skimming attacks. Even the issue of least concern among the seven – supply chain attacks – is still a significant concern for one-half (50%) of respondents. See Figure 2.

Figure 2
Levels of Concern About Various Threat Types
Percentage of respondents grouped by levels of concern



Source: Osterman Research (2021)

In 2020, 45% of those surveyed had significant concern about a cyberattack on their website; that figure jumped to 61% in 2021.

We discovered some interesting differences between this year's and last year's survey results:

- **A big increase in concern about cyber issues**
  In 2020, 45% of those surveyed had significant concern about a cyberattack on their website; that figure jumped to 61% in 2021, a major increase. Similarly, significant concern about supply chain attacks increased from 28% of respondents in 2020 to 50% in 2021. Concern about Magecart attacks grew by 47% year-over-year.

- **Two new threat types were highly rated**
  We asked about two new threat types in the survey this year: 1) the security risk posed by using external third-party scripts running on a website or application, and 2) the ease with which bad actors can abuse client-side scripts. We did not ask about these issues in previous surveys and have no comparative data. However, the level of significant concern about these two issues is similar to what we found for the top two issues in Figure 2, and significantly higher than all of the concerns we discovered in the 2020 survey.

CONSEQUENCES OF A CYBERATTACK REMAIN IMPACTFUL

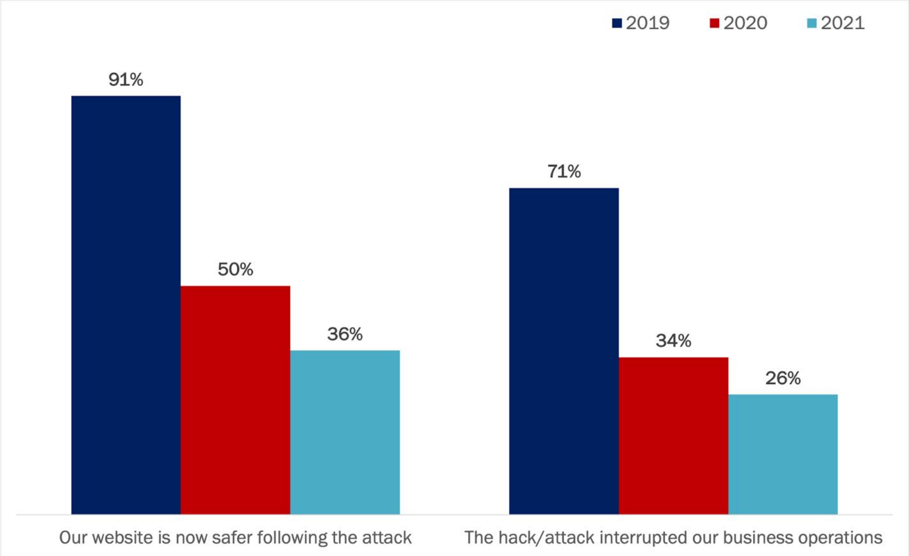
Respondents reported two consequences of cyberattacks against their organization's web applications:

- More than one third (36%) of respondents said that their organization's website is now safer following the attack, which indicates that they put in place technologies and/or processes to prevent similar attacks in the future.
- Slightly more than one-quarter (26%) of respondents told us that the attack interrupted their business operations.

See Figure 3 which provides a three-year view of these two consequences.

Almost 60% of respondents are concerned about the security risk posed by the use of external scripts running on their website.

Figure 3
Consequences From a Cyberattack of a Website
Percentage of respondents



Source: Osterman Research (2021)

Here's how the 2021 survey compares to the results of the previous two years:

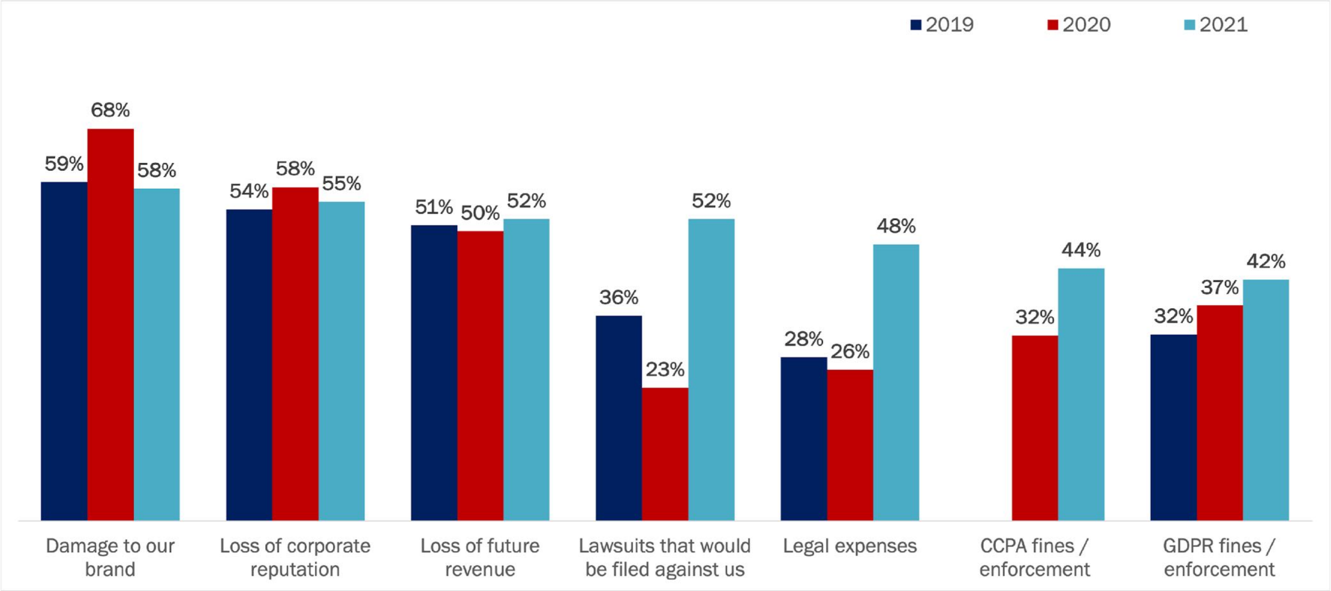
- **Websites are becoming less secure after attacks**
  Over time, less is being done to increase security for an organization's website after a cyberattack. For example, in 2019, 91% of respondents told us their websites were safer after an attack because of steps that were taken to address the vulnerabilities and other security problems. However, this figure dropped to 50% in 2020 and just 36% this year. Based on the three-year trend, fewer organizations are leveraging security incidents to resolve security weaknesses and vulnerabilities on their website.
- **Cyber resilience is improving**
  The percentage of organizations that told us that an attack interrupted their business operations declined, which suggests that organizations are improving their web application resilience. From a high point of 71% in 2019 to 34% last year and 26% this year, web application resilience is trending in the right direction.

BUSINESS CONSEQUENCES OF A DATA BREACH

Respondents were rightly concerned about the consequences of a major data breach occurring as a result of malicious client-side scripts running on their organization's website. The top three consequences that were cited are brand damage, loss of corporate reputation and loss of future revenue (see Figure 4).

Respondents were most concerned about brand damage, loss of corporate reputation and loss of future revenue as a result of a data breach.

Figure 4
Consequences of a Major Data Breach
Percentage of respondents indicating a major or huge problem



Source: Osterman Research (2021)

These three consequences have ranked as the areas of highest concern over the three years we have conducted this survey, but brand damage and loss of corporate reputation are less of a consequence in 2021 than they were in 2020. Across all of the ratings for every respondent and every consequence in this question, 50% of all answers indicated a "major" or "huge" problem, and only 6% indicated that any of these issues would not be a problem.

That said, we did find some variations in the data year-on-year including:

- **Two legal consequences increased the most**
  Lawsuits and legal expenses, which were considered the least important in last year's survey, are now the fourth and fifth most serious consequences of a data breach. By contrast, CCPA and GDPR fines/enforcement are now the least serious consequences. While these changes have affected relative positioning in Figure 4 above, the percentage of respondents indicating that these four issues carry significant weight has actually increased in every case, with the greatest increase seen in the two legal consequences.

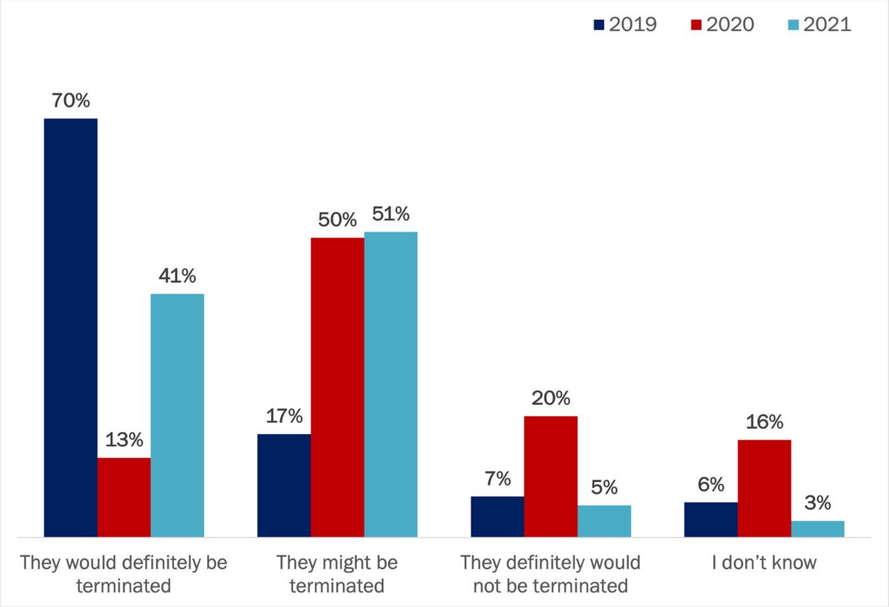
- **GDPR the least important issue**
  We found that GDPR is the least important issue in the year's survey and believe there are a couple of reasons for this. First, survey respondents were exclusively from the United States. The impacts of GDPR are less relevant for a US audience, particularly for those not transacting with data subjects in the European Union. Second, European regulators have factored the impact of the health pandemic into enforcement fines over the past year, and such discounted fines may have served to neutralize the threat of GDPR in the eyes of many.

PERSONAL CONSEQUENCES OF A MAJOR DATA BREACH

In addition to the consequences of a data breach at the organizational level, such as loss of business reputation, data breaches also carry personal consequences for those whose responsibility it is to protect against them. At the vast majority of organizations, the person responsible for externally facing website code would be likely to lose their job following a data breach caused by vulnerable scripts. For two-fifths of organizations, it would "definitely" lead to termination, and in just over one-half, it "might" lead to termination. See Figure 5.

In addition to causing business losses, data breaches also carry personal consequences for those whose responsibility it is to protect against them.

Figure 5
Consequences of a Major Data Breach on Job Roles
Percentage of respondents



Source: Osterman Research (2021)

In summary, there is much greater clarity this year that the people responsible for an organization's externally facing web properties would be likely to lose their job due to a data breach.

Significant Use of Shadow Code

In this section, we define Shadow Code and look at its usage characteristics.

WHAT IS SHADOW CODE?

Organizations have recognized the need to continue moving toward digital transformation, especially after they rapidly had to find new ways of engaging with customers, prospects, partners, and members of their software supply chain in 2020. However, speed-to-market is compromised when developers must write everything themselves. To do so requires developers on staff with a wide-range of skill sets, and even then, it just takes too long. Instead, leveraging existing open-source libraries and third-party code increases the speed of development and enables developers to be more responsive to rapidly changing business requirements.

The problem, however, is that the organizations whose websites are using third-party code are now at the mercy of the security reviews and validation—or lack thereof—of the entities that are supplying this code. These unvetted external scripts are collectively referred to as "Shadow Code", and they carry two major security risks:

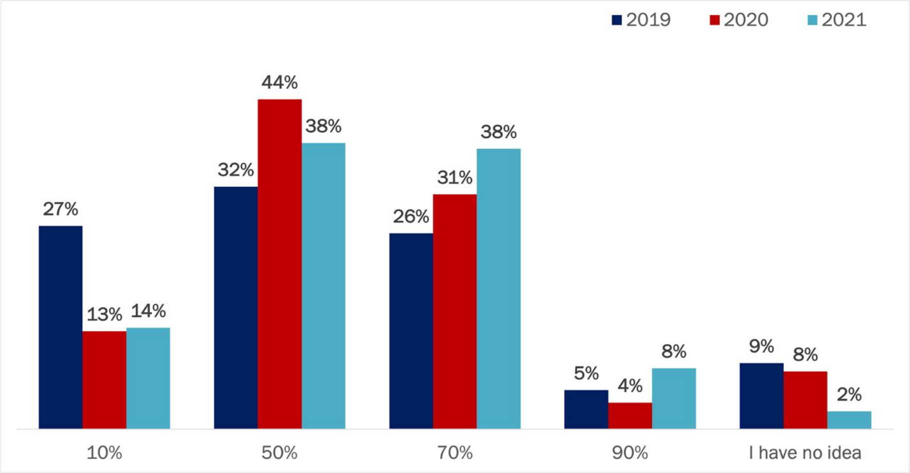
- First, malicious code could be introduced to the web application through an attack on a software supply chain vendor or the application itself by attacking a known vulnerability in the third-party code.
- Second, the attack surface of the organization is now increased, thus elevating the risk of data breaches. This hampers website owners' ability to comply with data protection regulations, and the overall risk to the organization using this code increases.

> ***About 70% of the typical website is comprised of third-party code.***

SHADOW CODE REMAINS A RISK

About 70% of the typical website is comprised of third-party code, although this varies widely by organization and industry. For the three years of this survey, we have asked respondents about the percentage of Shadow Code that the typical website contains. The good news is that most respondents *understand* the prevalence of Shadow Code; now, it's time to *address* the Shadow Code risk.

Figure 6
Perceived Use of Third-Party Code on a Typical Website
Percentage of respondents



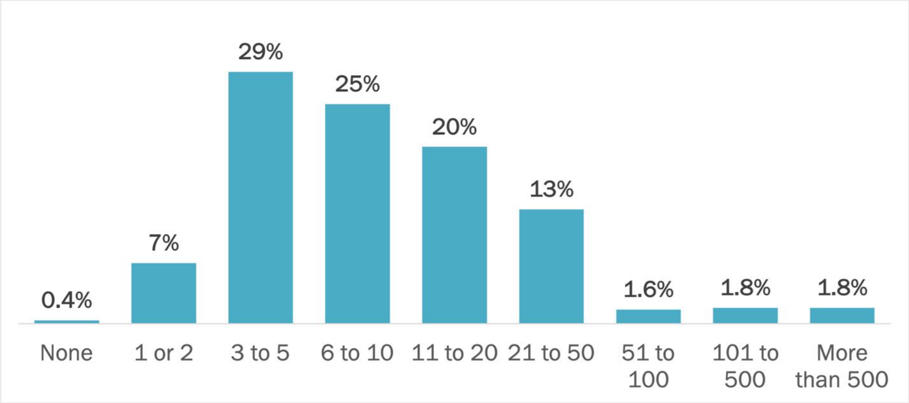
Source: Osterman Research (2021)

SIGNIFICANT USE OF THIRD-PARTY SCRIPTS

All but two respondents indicated that their organizations were using third-party scripts on their website, with over half saying that between three and ten scripts were in use on their websites. Slightly more than 5% of respondents said their organization’s website used more than 51 scripts, including almost 2% who said more than 500 scripts were in use. See Figure 7.

Over 99% of organizations use at least one third-party script.

Figure 7
Use of Third-Party Code on Respondents’ Websites
Percentage of respondents

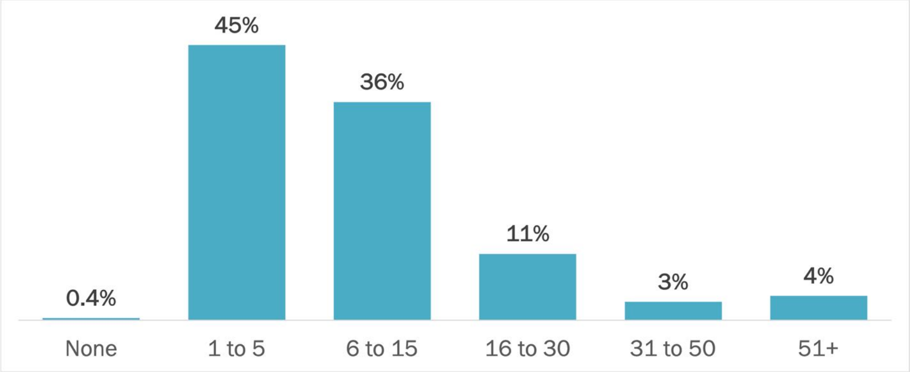


Source: Osterman Research (2021)

SOFTWARE SUPPLY CHAIN PARTNERS ARE VERY COMMON

Almost all organizations use supply chain vendors or partners for third-party code. The survey found that 45% of respondents believe that scripts from between one and five partners are in use, followed by 36% that believe the number is between six and 15. Four percent of respondents say they use 51 or more partners, a number which increased four times in the 2021 survey compared to 2020. The actual number is likely to be significantly higher, however, as first-party partners obtain code from their partners, increasing the length of the software supply chain. Partners' dependence on other partners for code may be undisclosed and is likely not appreciated by developers. See Figure 8.

Figure 8
Number of Software Supply Chain Vendors/Partners in Use
Percentage of respondents



Source: Osterman Research (2021)

Over 99% of organizations use supply chain vendors or partners for third-party code, who may themselves obtain code from their partners.

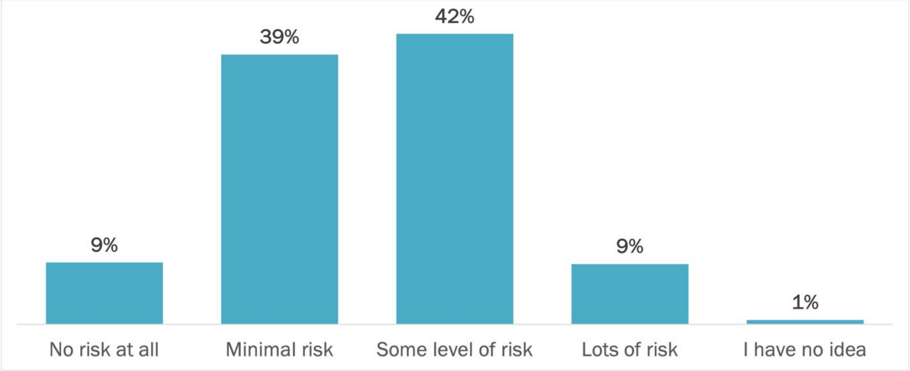
Risks and Trust with Shadow Code

Organizations that use Shadow Code should have good visibility and insight into the potential security risks that come with it. In this section, we consider the risks of Shadow Code and trust in third-party partners.

RISKS OF SHADOW CODE

The majority of respondents believe there is "some level of risk" or "lots of risk" in running third-party code on their website. Less than half believe the risk to be minimal or non-existent. See Figure 9.

Figure 9
Level of Security Risk Posed by Running Shadow Code
Percentage of respondents



Source: Osterman Research (2021)

Not surprisingly, the level of risk posed by running Shadow Code varies with the primary purpose of the website. Respondents with the following three primary purposes were more likely to perceive higher levels of risk:

- **Media and entertainment**
  Media and entertainment for customers to purchase digital media, play, meet others (e.g., dating apps), etc. Among these respondents, 57% saw "some" or "lots" of risk. Websites of this nature hold vast quantities of personal data, and in the case of dating apps, highly sensitive data.
- **Financial services**
  Financial services for customers to manage accounts. 54% of respondents saw "some" or "lots" of risk. Compromised financial accounts can lead to theft of funds and loss of trust in a financial institution, both of which can be difficult to recover from.
- **Consumer and industrial e-commerce**
  51% of respondents at organizations offering e-commerce websites for consumer and industrial customers for purchasing products and services also saw higher levels of risk. Compromised accounts on e-commerce websites can be used to steal credit card numbers or loyalty points, or to purchase gift cards or products for subsequent resale.

Respondents with the lowest level of risk assessment worked for organizations where the primary purpose of the website was gaming or delivery services. In short, respondents that operate websites that manage sensitive personal or financial information perceived the highest levels of risk from the use of Shadow Code.

AWARENESS OF RISKS OF SHADOW CODE

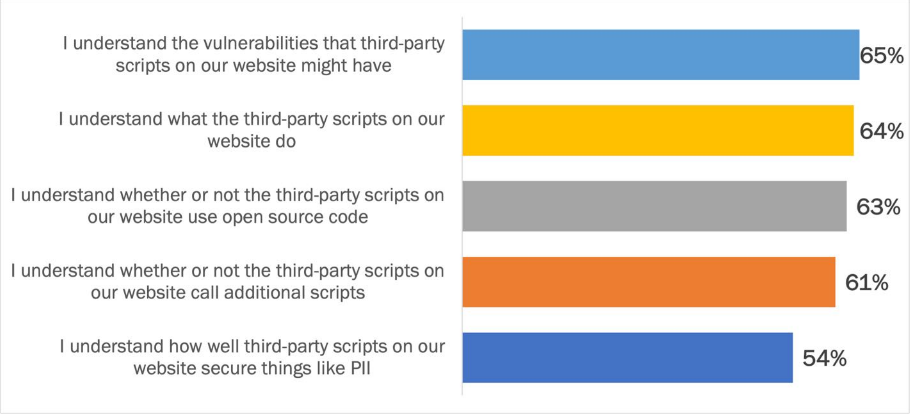
An average of almost two-thirds of respondents believe they have a good level of understanding of four risk factors associated with Shadow Code on their website:

- 65% understand the presence of possible vulnerabilities from third-party scripts
- 64% have a thorough understanding of how third-party scripts operate.
- 63% understand the use of open-source code.
- 61% know whether additional scripts are called by first party scripts. B
- 54% understand how third-party scripts secure things like personally identifiable information (PII)

To summarize our findings, between one third and almost one half of respondents do not have a good level of understanding of these five risk factors. Given the damage that third-party code can do, this is a serious issue that decision makers need to address. See Figure 10.

> ***Between one third and almost one half of respondents do not have a good level of understanding of the risk factors associated with Shadow Code on their website.***

Figure 10
Awareness of the Risks of Shadow Code
Percentage of respondents indicating “agree” or “strongly agree”



Source: Osterman Research (2021)

In correlating these answers with other questions, we discovered two important issues:

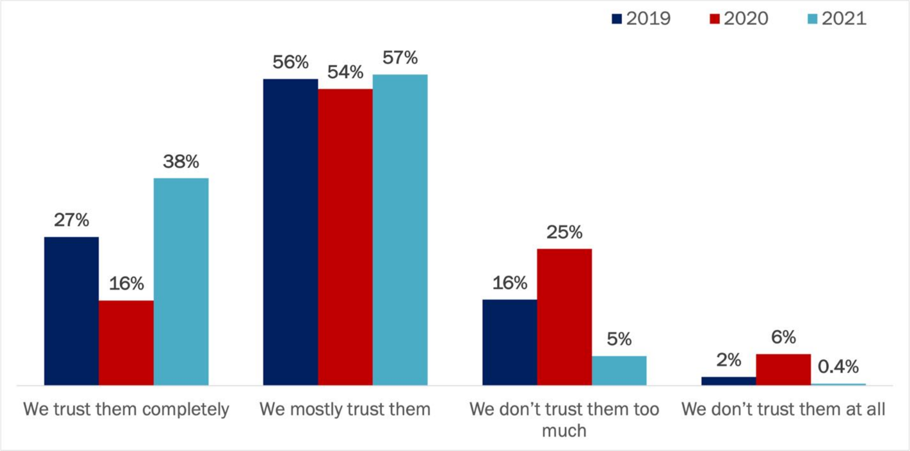
- **Variation by primary purpose**
First, respondents working in organizations where the primary purpose of the website is e-commerce, financial services, or travel and hospitality claimed a much higher understanding of all five risk factors than respondents working in the areas of media/entertainment, gaming or delivery services. For the first three, an average of 48% of respondents said they had a good level of understanding across all five factors, compared to an average of just 30% for the other three.
- **Little variation in the pattern of response for some**
Many decision makers felt similarly concerned about all of the issues presented in Figure 10. These respondents did not consider one issue to be substantially worse or better than the others, which suggests that they may not even know where to start to address their Shadow Code problem.

TRUST IN THIRD-PARTY PARTNERS

Software supply chain partners can definitely be the source of security threats in third-party client-side scripts. However, respondents in this year’s survey have fairly high levels of trust in the security of their partners’ code. The percentage of respondents indicating trust at the “complete” and “mostly” levels were at the highest points in the three years the survey has been conducted, and reversed the decline seen from 2019 to 2020. Respondents indicating complete trust in partners more than doubled from 16% last year to 38% this year, the largest increase to date. See Figure 11.

> ***Supply chain partners may call on code from their partners, lengthening the software supply chain and increasing business risk.***

Figure 11
Level of Trust for Partners Not to Be the Source of Security Threats
Percentage of respondents



Source: Osterman Research (2021)

Although organizations have increasing trust in their third-party partners, the supply chain risk often extends beyond this. Partners themselves frequently call on code from their own partners, which might be undisclosed.

The risks here should not be underestimated as the following examples will demonstrate:

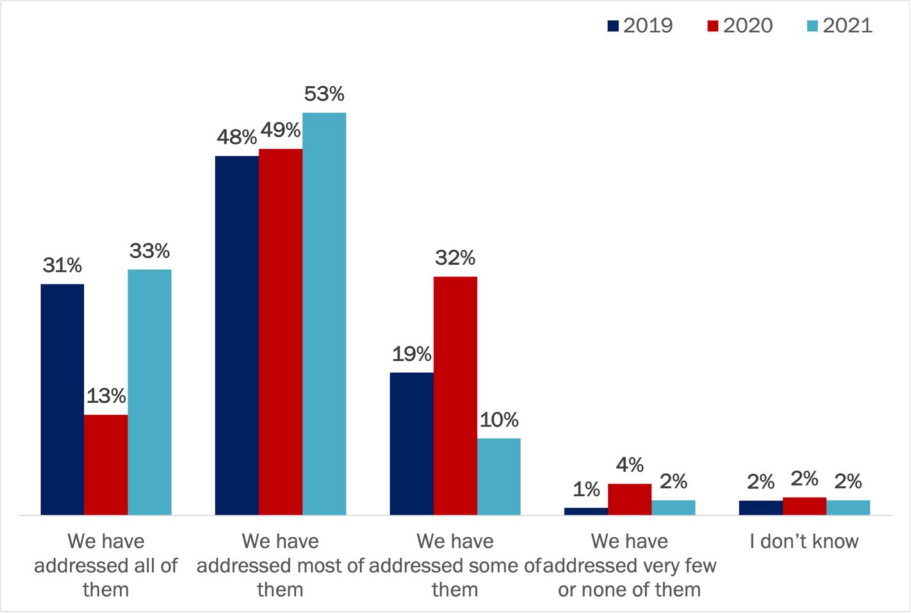
- **SolarWinds**
  A major software supply chain attack was detected at SolarWinds in December 2020, which compromised more than 18,000 organizations, including security vendors and government agencies that should be among the most highly protected organizations in the world.
- **Kaseya**
  In July 2021, Kaseya was involved in a supply-chain ransomware attack. Because its solutions are used by managed service providers, this attack impacted potentially tens of thousands of client organizations.

Both SolarWinds and Kaseya have suffered supply chain attacks in recent years.

HIGH RATE OF ADDRESSING KNOWN VULNERABILITIES

Respondents claim to have addressed "all" (33%) or "most" (53%) of the vulnerabilities that may be present in the third-party client-side scripts that run on their organization's websites. The percentage of respondents in both groupings has increased from last year's result, with the "all" option increasing significantly, from 13% to 33%. Only 16% in total have addressed only "some" or "very few" to "none" of these vulnerabilities, or just don't know the current state. See Figure 12.

Figure 12
Extent to Which Organizations Have Addressed Known Vulnerabilities from Third-Party Scripts
Percentage of respondents



Source: Osterman Research (2021)

Addressing known vulnerabilities is essential, but there are two additional issues to consider:

- **Protecting against unknown vulnerabilities**
  Unknown vulnerabilities, zero-days, software supply chain compromises, and new vectors are all possible pathways for cybercriminals to execute an attack. These threats are much more difficult to protect against.
- **Time to detect vulnerabilities**
  Third-party code suppliers issue warnings and update code frequently as new vulnerabilities are identified. Organizations are running blind if they do not have security tools in place to triangulate code vulnerability updates or the ability to rapidly distribute new updates. This must cover both known third-party code and undisclosed code that comes from supply chain partners.

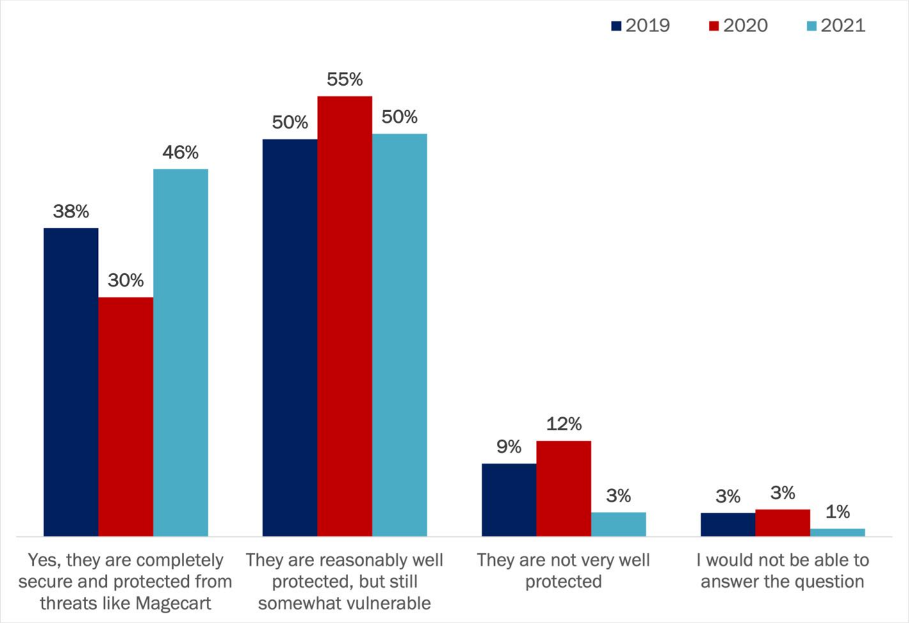
Addressing known vulnerabilities is essential, but it is equally important to protect against unknown vulnerabilities and reduce the time it takes to detect them.

COMPLIANCE IS IMPROVING

We have asked the following question over the three years of the survey: “If you were asked by your senior management if your externally-facing web properties are secure, and thus compliant with GDPR, the California Consumer Privacy Act and similar types of data privacy regulations, what would your answer be?”

Fewer than half of respondents to this year’s survey would be willing to tell senior management that their externally facing web properties are completely secure and protected from threats like Magecart and in compliance with GDPR and CCPA. See Figure 13.

Figure 13
Extent of Compliance with Data Protection Regulations Such as GDPR and CCPA
Percentage of respondents



Source: Osterman Research (2021)

Data privacy regulations — including GDPR in Europe, CCPA/CPRA in California and others — impose important requirements on website operators. These regulations address issues like protection for personal data and personally identifiable data, and the rights that data subjects might have for the protection and management of their data. An inability to comply with these regulations can lead to serious consequences like data breaches, but also significant costs to an organization's reputation and from financial penalties from regulators.

> ***Fewer than half of respondents would be willing to tell senior management that their externally facing web properties are completely secure.***

Misplaced Trust, Hidden Risk

From the answers in the previous section, it appears that organizations are on their way to solving the problem of Shadow Code. However, when we looked below the surface, we uncovered a disconnect between respondents' beliefs and organizational practices. In this section, we look at how organizations lack the operational security processes and technologies to support a position of high trust in third-party code providers.

HIGH RATE OF CHANGE IN THIRD-PARTY SCRIPTS, BUT LOW ADOPTION OF SECURITY REVIEW PROCESSES

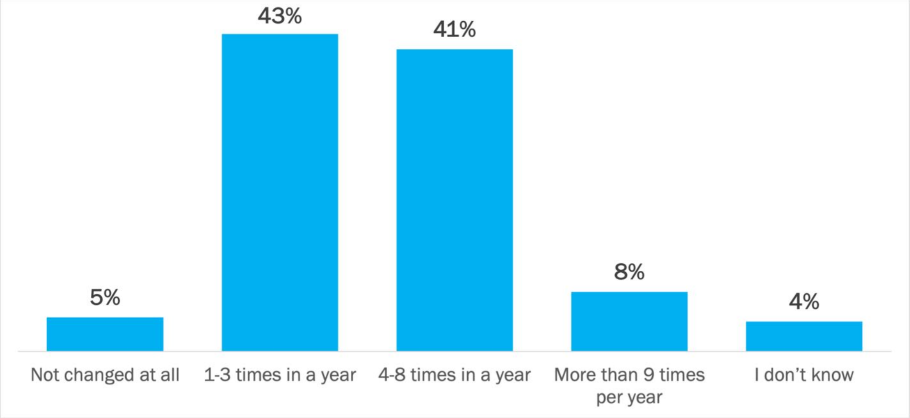
Over half of respondents state that third-party scripts running on their web properties change four or more times every year (Figure 14). However, only one quarter of respondents perform a security review process for every script modification (Figure 15). Most respondents either run a security review process for only some updates (35%) or only when a new script is initially deployed (29%). The remainder never run a security review process on any third-party scripts (11%).

In combination, these findings are alarming for a couple of reasons:

- **Risks are invisible**
  Supply chain partners may introduce updated or replacement script libraries without notifying organizations of the changes. Even if an organization has high trust in their primary software supply chain partners, the undisclosed inclusion of code from other partners can put the primary organization's website at serious risk.

- **Newer code introduces new risk**
  Code is often updated to improve features, functions or performance, but that does not necessarily mean improved security. Updates can introduce new weaknesses or call other third-party libraries that have introduced new weaknesses through updates. Organizations that perform a security review only on initial deployment wrongly assume that their security position does not change.

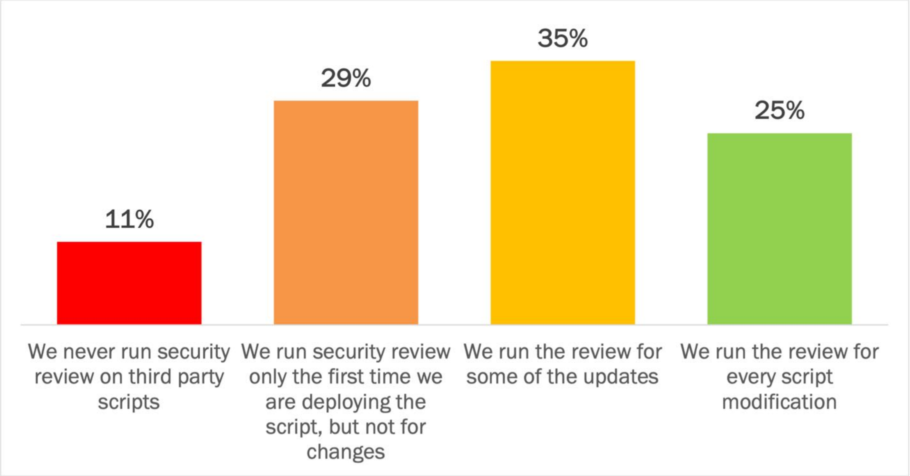
Figure 14
Number of Updates and Changes in Third-Party Scripts Each Year
Percentage of respondents



Source: Osterman Research (2021)

> ***Code is often updated to improve features, functions or performance, but that does not necessarily mean improved security.***

Figure 15
Security Review Approach for Third Party Scripts
Percentage of respondents



Source: Osterman Research (2021)

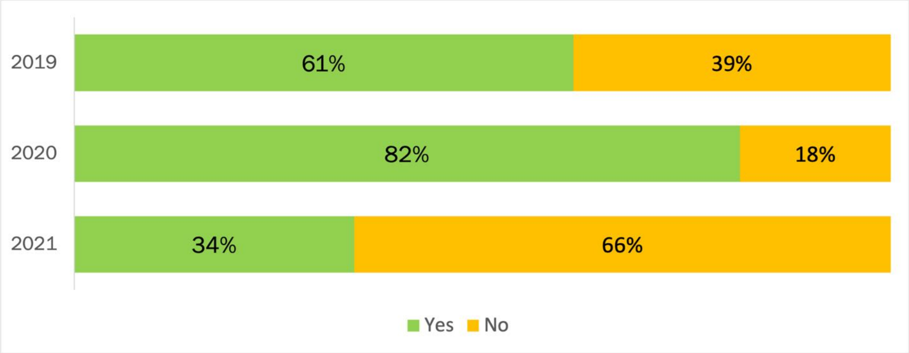
These two questions were not asked in the previous surveys, hence there is no comparative data available to indicate a year-over-year trend. Nonetheless, reviewing every script modification is a best-practice approach that 75% of respondents are not yet following.

Assessments of security posture are often outdated due to frequent code changes.

LOW RATES OF AUTOMATIC DETECTION

Over the past year, organizations have taken a backwards step in their ability to detect changes or updates made on their website that could potentially lead to a security problem. A startling 66% of respondents cannot detect changes or updates, compared to 18% in 2020 and 39% in 2019. See Figure 16.

Figure 16
Ability to Detect Security Problems Due to Changes or Updates on a Website
Percentage of respondents



Source: Osterman Research (2021)

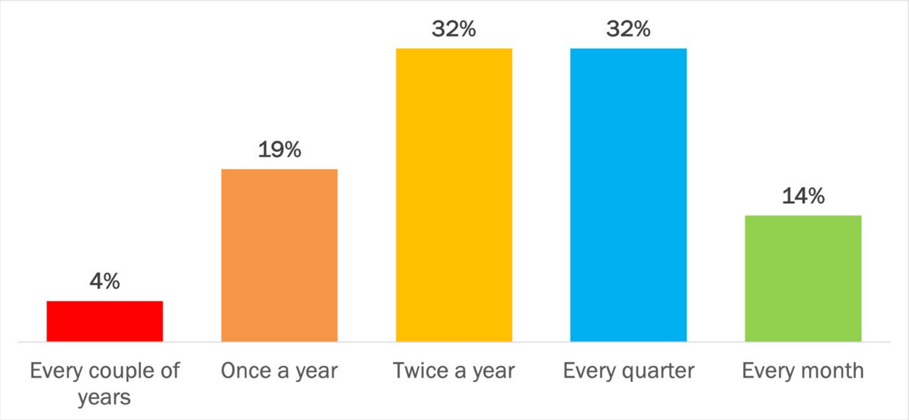
The code that runs websites is dynamic, due to both internal and supply chain code changes. Not having the ability to detect security problems as code changes means that organizations:

- **Lack up-to-date awareness of security posture**
  Assessments of security posture are often outdated because of frequent changes to code. This offers a false sense of assurance to developers and website operators that their site is secure.
- **Unwittingly introduce compromised code**
  If an update to third party code impacts website security, without review, organizations might realize their risk only when their website suffers a cyberattack.

PENETRATION TESTING TOO INFREQUENT TO BE OF ANY USE

Almost all respondents' organizations make use of pentesting, but only 14% run tests internally or externally every month. Almost two-thirds run tests every 3 to 6 months. Testing so infrequently offers a low likelihood of identifying emerging threats before they can be exploited. See Figure 17.

Figure 17
Frequency of Pentesting
Percentage of respondents



Source: Osterman Research (2021)

Manually reviewing the security impact of code changes on a website is too slow to account for the code's rate of change.

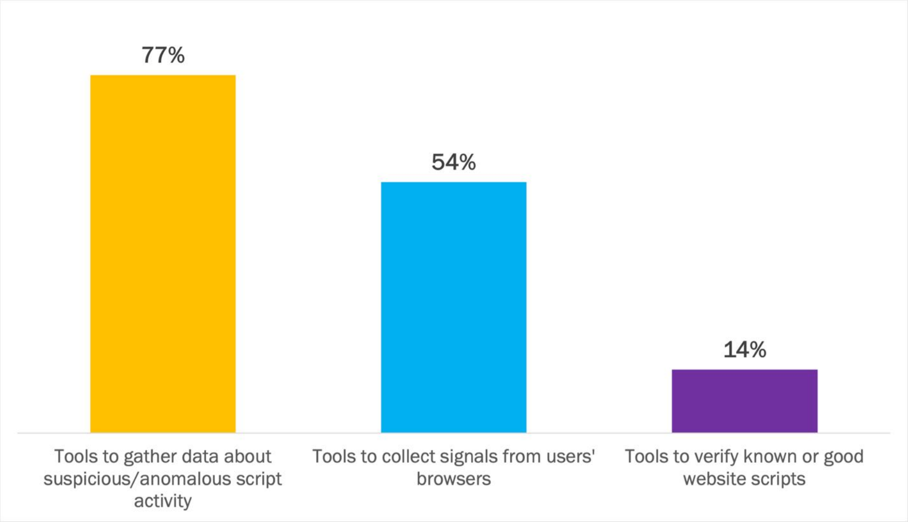
While penetration testing has a number of benefits and is an important tool for ensuring the security of applications and code in many situations, the way it is used makes it unreliable in identifying vulnerabilities from Shadow Code. The reasons for this include:

- **Checkbox exercise only**
  Many organizations treat pentesting merely as a checkbox exercise to demonstrate compliance, rather than as something substantive and fundamental to security.
- **Human labor alone cannot keep up with the rate of change**
  Manual review of the security impact of code changes on a website is too slow to account for the code's rate of change. The permutations of even a single code change can easily overwhelm the ability of pentesters to identify downstream impacts.

INSUFFICIENT TOOLS TO MONITOR SCRIPT ACTIVITY

Respondents indicated varying usage of three different tools to gather data about script activity. Tools to gather data about suspicious/anomalous script activity are the most common (77% of respondents), followed by tools to collect signals from users' browsers (54%). See Figure 18.

Figure 18
Use of Tools for Identifying Script Activity
Percentage of respondents for each tool

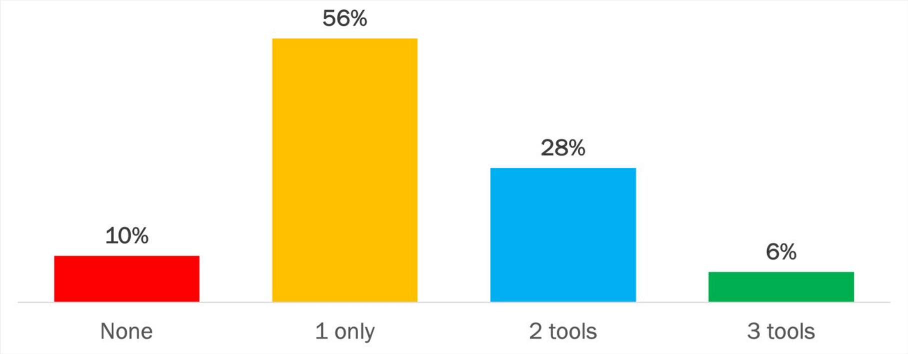


Source: Osterman Research (2021)

Only 6% of respondents use a tool in all three categories, with 56% using tools only in a single category and 10% using none of the tools about which we inquired. See Figure 19.

> ***A lack of tooling to identify script activity introduces systematic blindness to the threats hidden in an organization's web properties.***

Figure 19
Spread of Tools Used for Identifying Script Activity
Percentage of respondents



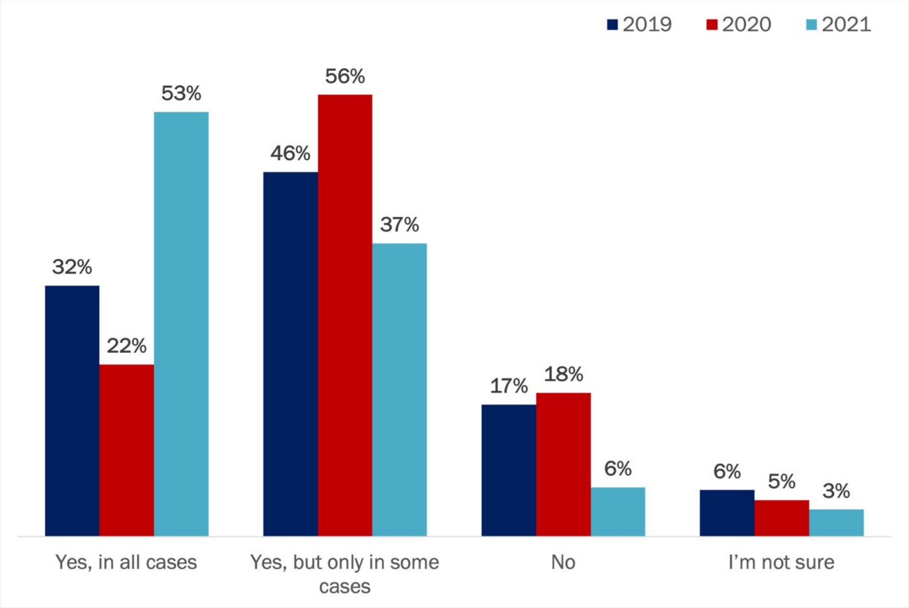
Source: Osterman Research (2021)

A lack of tooling to identify script activity introduces systematic blindness to the threats hidden in an organization's web properties. It also makes security teams blind to where those threats are actively undermining security precautions, where they may be exfiltrating data, or where they are compromising user activity.

SHUTTING DOWN SUSPICIOUS SCRIPTS

The ability to shut down third-party scripts that seem anomalous or suspicious is key for protecting web properties from malicious behavior, data breaches, ransomware attacks and other cybersecurity threats. Over the past year, there has been a shift in the authority given to the security team for shutting down such scripts. We saw the greatest gain among organizations that give the security team complete autonomy to shut down anomalous scripts without first receiving approval from higher ups: this grew from just 22% of organizations in 2020 to 53% in 2021. See Figure 20.

Figure 20
Extent to Which the Security Team Has the Authority to Shut Down Suspicious Scripts
Percentage of respondents



Source: Osterman Research (2021)

While security teams can benefit from increased authority, this alone represents a failure of process. Specifically:

- **Security review processes should be the preference**
  The use of robust security review processes should catch issues with third-party scripts before they are used on externally facing web properties. Allowing script changes to propagate to web properties without a security review represents a less-than-optimal approach to security. It's a bit like using the emergency brake to stop a car because no one first checked if the primary brake system was operational.

- **Unknown cascading effects**
  Shutting down third-party scripts on operational web properties will often have an unknown effect on functionality and performance, potentially compromising the web experience for customers and prospects. In a worst-case scenario, it could weaken other security precautions and lead to significant losses of revenue, for example, if customers can no longer complete a transaction on the site.

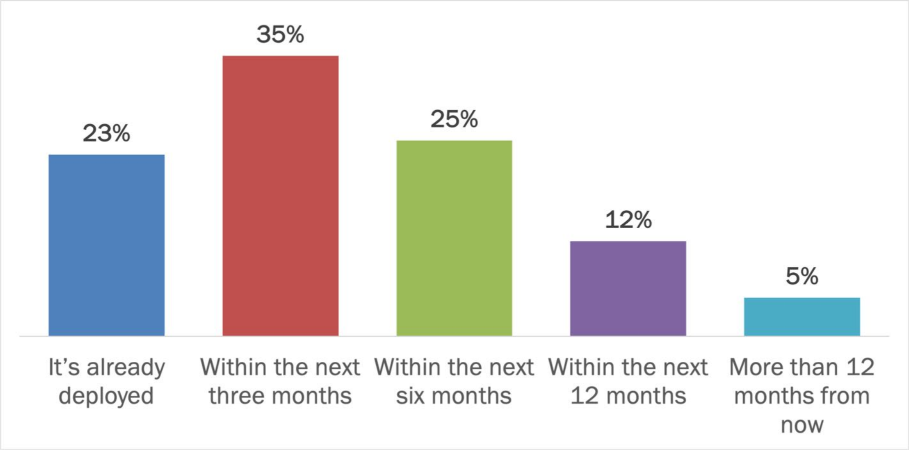
The use of robust security review processes should catch issues with third-party scripts before they are used on externally facing web properties.

The ability to shut down suspicious scripts is an essential capability and we welcome the greater proportion of security teams that are able to do so. That said, we would prefer to see organizations using more refined tools for script evaluation, assessment and verification rather than relying on brute force security approaches alone.

TIMEFRAME FOR DEPLOYING SOLUTIONS

Three-quarters of respondents intend to purchase solutions to address website script vulnerabilities in the next twelve months. One third of respondents intend to deploy such a solution within the next three months, and one quarter within a three-to-six-month timeframe. Of the overall respondent base, just under one quarter say they have already deployed solutions in this area. See Figure 21.

Figure 21
Timeframe Intent for Deploying Solutions to Address Website Script Vulnerabilities
Percentage of respondents



Source: Osterman Research (2021)

75% of respondents intend to purchase solutions to address website script vulnerabilities within the next 12 months.

SIGNIFICANT NEED FOR EDUCATION

When asked to list security vendors that they would consult when addressing client-side website vulnerabilities, respondents listed more than 200 vendors in total. However, most of these vendors lack solutions to address client-side website vulnerabilities. For example, five vendors that sell general security solutions were mentioned by 50% of respondents—Cisco, McAfee, IBM, Microsoft, and Symantec—none of which can actually help in this area.

In selecting vendors to assist with addressing website vulnerabilities introduced by Shadow Code, decision makers need to be very clear that the vendors they approach can actually do something to help.

It's also important to note that only 29% of respondents told us they have evaluated solutions to address website script vulnerabilities during the past 12 months. 71% have not carried out this process. Based on the risks highlighted in this survey, organizations that have not already evaluated solutions and are planning on deploying a solution within the next three months need to add urgency to their vendor assessment and selection processes.

Summary

For the third year in a row, this research has looked at the awareness of risks from Shadow Code on organizations' websites. There is strong awareness of the consequences of a successful cyberattack against an organization's websites, but the evidence indicates a false sense of safety from these attacks. Organizational security review processes are insufficient, capabilities to automatically detect changes have low adoption and other means of assessing threats from code vulnerabilities are not up to the task. Businesses need to urgently review their efficacy in detecting and managing risks that third-party scripts and open-source libraries introduce to web applications.

Sponsored by PerimeterX

PerimeterX is the leading provider of solutions that protect modern web apps at scale. Delivered as a service, the company's Bot Defender and Code Defender solutions detect risks to your web applications and proactively manage them, freeing you to focus on growth and innovation. The world's largest and most reputable websites and mobile applications count on PerimeterX to safeguard their consumers' digital experience. PerimeterX is headquartered in San Mateo, California and at www.perimeterx.com.

perimeterx

www.perimeterx.com

@perimeterx

info@perimeterx.com

+1 650 620 7800

Osterman Research does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.