Osterman Research
SURVEY REPORT

Survey by Osterman Research
Published **August 2020**
Sponsored by **PerimeterX**

Shadow Code: The Hidden Risk to Your Website

Application Security Risk Survey 2020

Executive Summary

Osterman Research conducted a major, in-depth survey during May and June 2020 to uncover the extent and impact of third-party scripts and open-source libraries used in web applications across organizations spanning multiple verticals. These scripts and libraries – often added without approvals or security validation – introduce hidden risks into the organization and make it challenging to ensure data privacy and to comply with regulations. Collectively referred to as "Shadow Code", these scripts might be used for ad tracking, payments, customer reviews, chatbots, tag management, social media integration or helper libraries that simplify common functions. The goal of this survey was to understand the hidden risks to the organization from Shadow Code.

This is the second annual report produced by Osterman Research on behalf of PerimeterX discussing the results of in-depth surveys on the use of Shadow Code in websites. The 2019 survey was conducted with 307 security professionals and developers, while the 2020 survey was conducted with 503 security professionals and developers. In order to qualify for these surveys, respondents had to be familiar with third-party scripts or scripts from third-party libraries in terms of how they are used in their organization's website(s). Moreover, the primary purpose of the website(s) operated by the organizations surveyed had to be one of the following in the 2020 survey:

- Retail/e-commerce for consumer or industrial customers
- Financial services for customers to manage their accounts
- Travel and hospitality
- Media/entertainment
- Gaming/online media
- Delivery services

Where there were significant differences between the results in the 2019 and 2020 surveys, this report highlights and discusses those differences.

Only eight percent of respondents report that they have complete insight into the third-party code that is currently running on their websites.

KEY TAKEAWAYS

Here are the key takeaways from the research:

- **Shadow Code remains a blind spot for most information security teams**
  Only eight percent of respondents report that they have complete insight into the third-party code that is currently running on their websites. This is down from 10 percent in 2019.

- **Trust in third-party script providers is eroding**
  Thirty-one percent of respondents report that they do not trust the providers of their third-party scripts, a significant increase from the 17 percent who lacked trust in their third-party scripts in the 2019 survey.

- **Information security teams lack necessary controls over website scripts**
  Only 22 percent of the respondents indicated that they or their teams have the full authority to shut down any suspicious script that they might find running on their website. This is down from 32 percent since 2019.

- **Confidence in website security is decreasing – most don't believe that their web properties are secure**
  Only 30 percent of survey respondents believe that their externally-facing web properties are completely secure from threats like Magecart attacks. In the 2019 survey, 38 percent reported that they thought their web properties were secure.

- **Most organizations know or suspect that their website has been hacked**
  Thirty-eight percent of respondents know for a fact that their corporate website was hacked (up slightly from 36 percent in 2019), and another 40 percent suspect this is the case.

- **Compliance with data privacy regulations such as CCPA remains low**
  Only 30 percent of respondents to the survey reported that their externally facing web properties are compliant with data privacy regulations.

- **The COVID-19 pandemic is slowing adoption of solutions**
  Currently, 34 percent of respondents have deployed solutions to address the Shadow Code risk. However, had the pandemic and the associated lockdowns and slowdowns not occurred, this number would have been much higher at 47 percent. This means that 28 percent of organizations that wanted to protect their web applications have been unable to do so due to COVID-19.

ABOUT THIS SURVEY REPORT

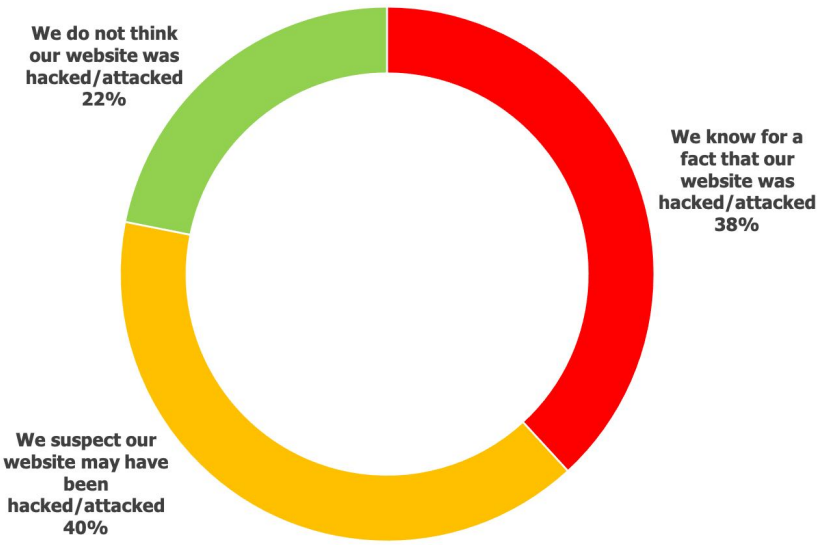
The survey and survey report were sponsored exclusively by PerimeterX; information about the company is provided at the end of this report.

Website Threats Abound

Our research found that 38 percent of those who are knowledgeable about their organizations' web properties know for a fact that their website has been hacked or attacked, as shown in Figure 1. Moreover, another 40 percent believe that their website has been hacked or attacked, although they lack the proof to verify their suspicion. Only 22 percent do not believe that their corporate website has been hacked or attacked.

38 percent of those who are knowledgeable about their organizations' web properties know for a fact that their website has been hacked or attacked.

Figure 1
Knowledge of Website Attacks



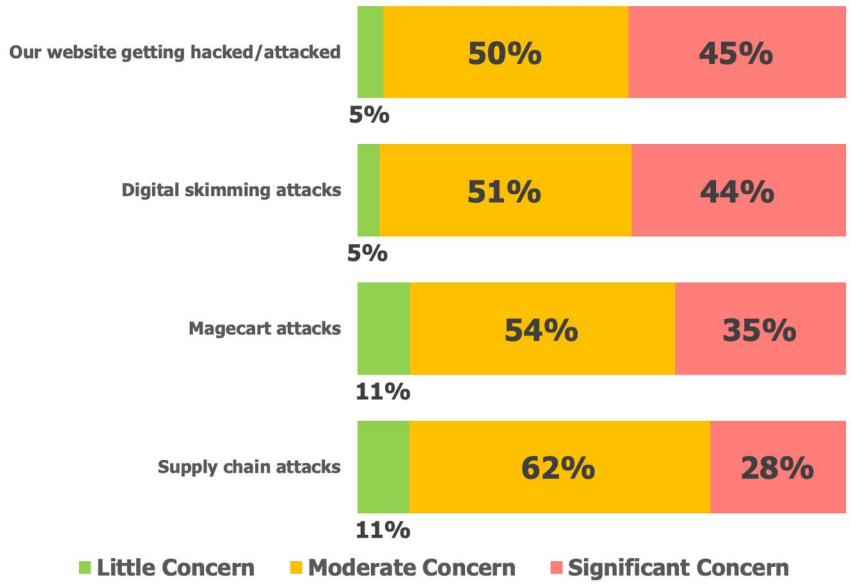
Source: Osterman Research, Inc.

Website attacks are common and increasing. SonicWall reported that attacks on web applications increased by more than 50 percent during 2019, and that more than 40 million such attacks occurred during that year[1]. Moreover, the Open Web Application Security Project (OWASP) has given web application component security risks their highest prevalence score on their Top 10 list of web application security issues[2].

THERE IS SIGNIFICANT CONCERN OVER THREATS

As shown in Figure 2, those knowledgeable about their organizations' web properties express a great deal of concern over various types of attacks and threats. For example, 45 percent are very concerned about their websites getting hacked or attacked and another 50 percent have a moderate concern about these threats. Decision makers are also deeply concerned about digital skimming attacks, Magecart attacks and supply chain attacks: 28 to 44 percent of respondents indicated that these attacks are a significant concern.

Figure 2
Levels of Concern About Various Threat Vectors



Source: Osterman Research, Inc.

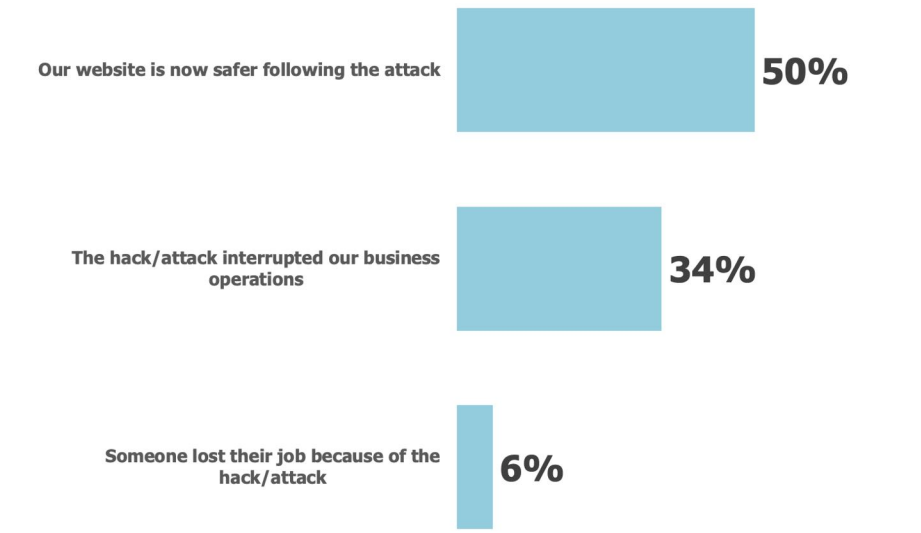
Website attacks are common and increasing.

THE CONSEQUENCES OF AN ATTACK

Not surprisingly, about 34 percent of organizations whose websites have been hacked or attacked report that they suffered an interruption in business operations, and six percent reported that at least one person in the organization was terminated as a result, as shown in Figure 3. Interestingly, however, 50 percent of organizations reported that their website is now safer following the attack, no doubt the result of remediation actions that helped organizations find vulnerabilities in their website code that were subsequently addressed.

[1] https://www.thesslstore.com/blog/cyber-security-statistics/#web-applications
[2] https://medium.com/@oliversild/third-party-components-the-largest-threat-to-web-security-23ac4714fd99

Figure 3
Consequences From the Hack/Attack of a Website



Source: Osterman Research, Inc.

The silver lining behind website attacks is that it really does wake up security and business decision makers about the dangers associated with website attacks. It frees up budgets to deploy the appropriate technologies and processes necessary to prevent future attacks, it greenlights new initiatives focused on improving security, it increases the level of scrutiny across the supply chain, and it delivers the appropriate degree of attention on preventing future attacks.

34 percent of organizations whose websites have been hacked or attacked report that they suffered an interruption in business operations.

Shadow Code Dominates Websites

WHAT IS SHADOW CODE?

Web developers leverage open source libraries and third-party code to innovate and keep pace with evolving business needs. Third-party scripts often introduce fourth-, fifth- and Nth-party scripts into the web application, creating a digital supply chain of code that is introduced without approvals or proper security validation. All of this is collectively referred to as Shadow Code.

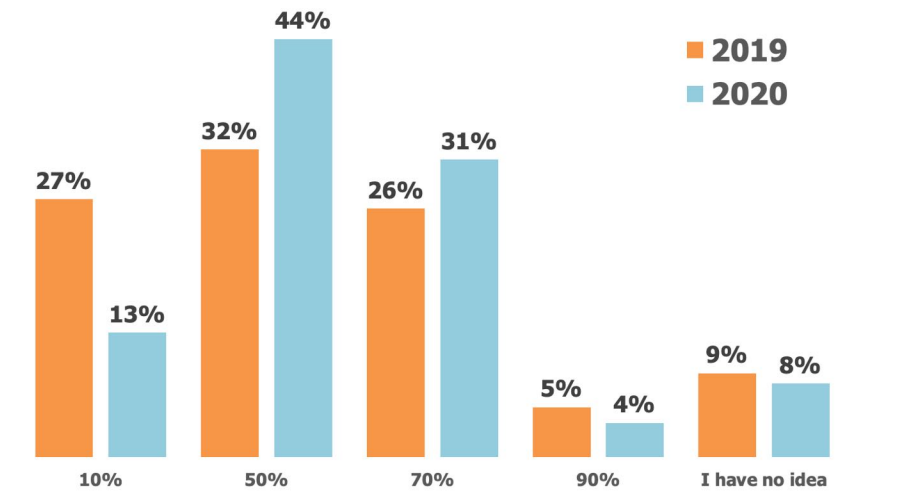
Shadow Code also includes malicious code that could get introduced into the web application through attacks on any of the supply chain vendors, or through a compromise of the application itself.

Shadow Code expands the attack surface for an organization, increases the risk of data breaches and makes it difficult to comply with data privacy regulations.

SHADOW CODE REMAINS A HIDDEN RISK

Independent analysis has confirmed that about 70 percent of the content on a typical website consists of third-party code, although this varies widely by organization and industry. However, as shown in Figure 4, the majority of decision makers believe the figure is somewhat lower than this. In the most recent survey, 57 percent of decision makers believe that the volume of third-party code is no more than 50 percent, while 31 percent believe the figure to be 70 percent.

Figure 4
Perceived Percentage of Typical Website Code That is Comprised of Shadow Code



Source: Osterman Research, Inc.

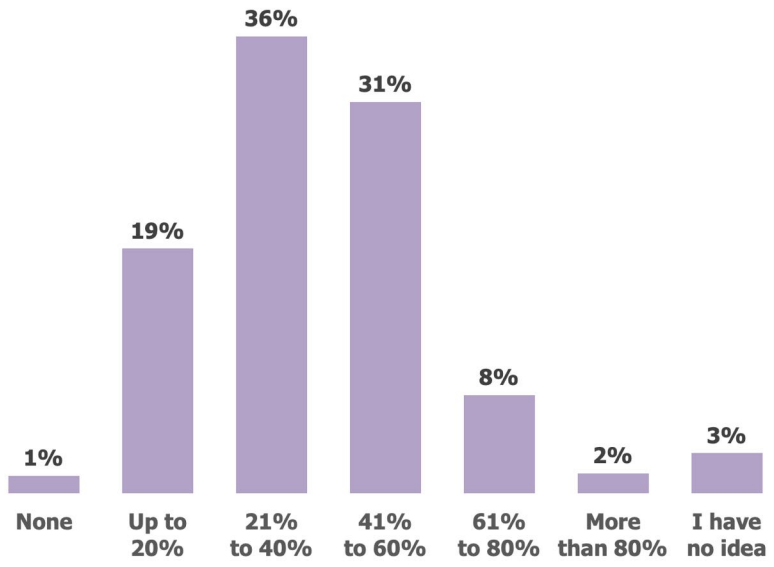
Interestingly, we found some significant differences between the 2019 and 2020 surveys, as shown above. The number of decision makers who believe that 50 to 70 percent of their website is third-party has jumped up 29 percent since 2019. In other words, awareness of Shadow Code is increasing in the industry.

Shadow Code expands the attack surface for an organization.

MOST HAVE UP TO 50 PERCENT THIRD-PARTY SCRIPTS ON THEIR WEBSITES

The data above shows responses to the amount of third-party code in websites in general. In the following question, however, we specifically asked about third party code on websites operated by the survey respondents' organizations. As shown in Figure 5, 10 percent of websites have more than 60 percent of their code represented by third-party scripts, and 41 percent of websites obtain more than 40 percent of their code from third parties. Only one percent of respondents indicated that all of the code on their websites is homegrown, while three percent of respondents have no idea how much Shadow Code is present. The last data point should be worrisome for security decision makers in those organizations, since not even knowing how much Shadow Code operates behind the scenes makes identification of the problems associated with it that much more difficult. We found that the average percentage of third-party scripts increased slightly from the 2019 to the 2020 survey: from 34.6 percent to 36.1 percent.

Figure 5
Percentage of Shadow Code That Runs on Corporate Websites



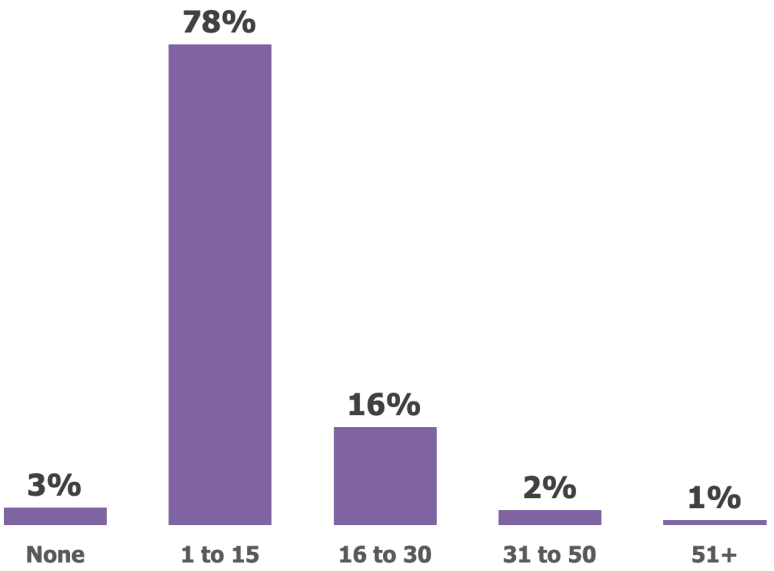
Source: Osterman Research, Inc.

MOST HAVE WEBSITE SUPPLY CHAIN PARTNERS

The vast majority of organization have supply chain vendors or partners on whom they rely for third party code, as shown in Figure 6. Most organizations have between one and 15 website supply chain vendors/partners, but 19 percent of organizations have more than 15. However, it is important to note that while website operators are dealing directly with various supply chain vendors, these vendors are also working with members of their own supply chain, and so the actual number of third-parties whose code is running on a website may be much higher than many decision makers consider.

The vast majority of organizations have supply chain vendors or partners, such as third-party providers of code.

Figure 6
Number of Website Supply Chain Vendors/Partners in Use



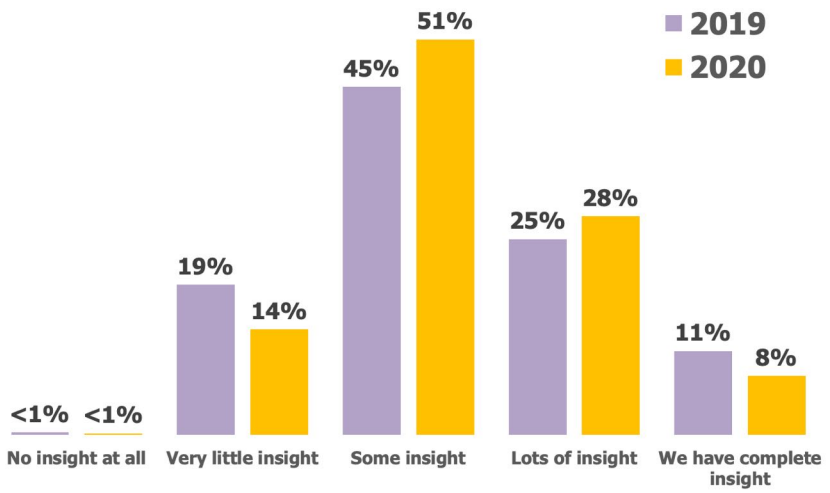
Source: Osterman Research, Inc.

Shadow Code Visibility and Insight is Not Where it Should Be

The level of insight about Shadow Code on the part of those knowledgeable about their organizations' web properties varies widely. As shown in Figure 7, about 14 percent of decision makers in the survey conducted this year has very little or no insight into the Shadow Code that operates on their corporate website. Fifty-one percent have what they believe to be "some" insight, while 36 percent have a significant amount or complete insight.

This lack of insight and visibility represents a major blind spot for organizations that makes it challenging to comply with data privacy regulations like the California Consumer Privacy Act (CCPA) or the General Data Protection Regulation (GDPR). Because these and other privacy statutes require website operators to securely collect, transmit and store personal information, if the operation of third-party code is not confirmed to be secure prior to its use, it could create a data breach that would put a website operator in jeopardy.

Figure 7
Level of Insight About Shadow Code That Runs on Corporate Websites



Source: Osterman Research, Inc.

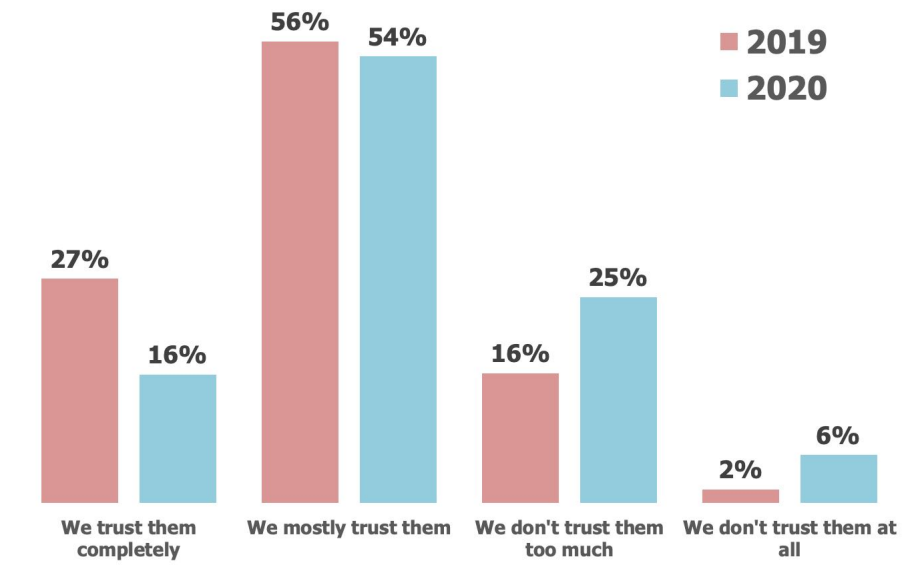
The level of insight about Shadow Code on the part of those knowledgeable about their organizations' web properties is not all that high.

Compared to the data from last year's survey, things are improving: fewer decision makers have very little or no insight into the Shadow Code used on their websites, and slightly more have either "some" or "lots" of insight. No doubt this improvement has been prompted by a combination of major data breaches and other incursions in web properties, as well as vendors' continued efforts at educating their potential customers about the dangers inherent in the poorly understood third-party scripts operating on their websites.

TRUST IS ERODING

The lack of insight into Shadow Code is complicated by the general lack of trust that website operators have of their business partners not to be the source of code that puts them at risk. As shown in Figure 8, the vast majority of organizations do not completely trust their business partners not to be the source of security vulnerabilities in the Shadow Code used in their websites. Only a fraction of website operators have complete trust in these partners.

Figure 8
Level of Trust for Partners Not to be the Source of Security Threats in Shadow Code



Source: Osterman Research, Inc.

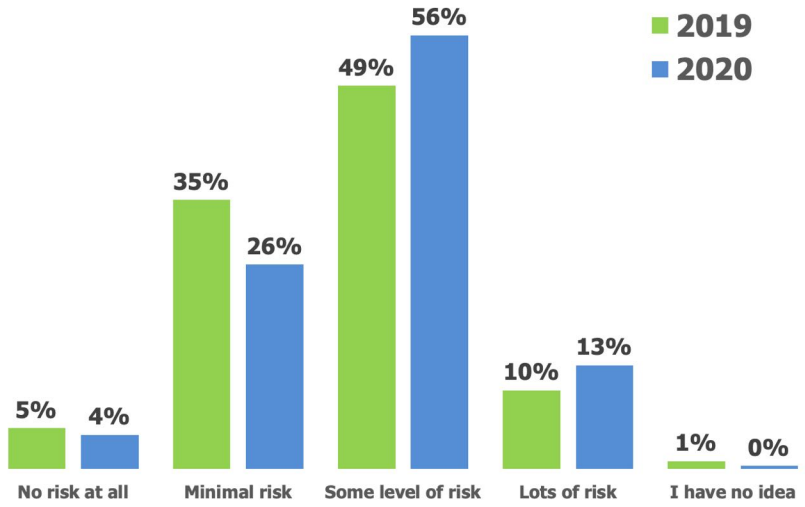
Interestingly – and perhaps not coincidentally – the level of trust discovered in the 2020 survey proved to be significantly lower than in the 2019 survey: whereas 27 percent of website operators had complete trust in their partners in 2019, that has dropped to just 16 percent this year. Add to that the fact that those website operators who have little or no trust in their partners has increased significantly year-on-year. This lack of trust, particularly in the context of the security of web properties that are critical to an organization's business, can lead to broken business relationships. On the plus side, however, it can also be the driver for helping decision makers to vet their third-party code providers more carefully, and can motivate them to investigate technologies to help them discover and address code vulnerabilities.

MOST ORGANIZATIONS UNDERSTAND THAT SHADOW CODE IS RISKY

Not surprisingly, many of those knowledgeable about their organizations' website properties do not have good insight into the third-party scripts that are running in their web properties, and not surprisingly most believe that Shadow Code poses significant to serious risks. As shown in Figure 9, more than 69 percent of those knowledgeable about their organizations' websites believe that Shadow Code poses at least some level of risk, and 13 percent consider the use of this code to be very risky. Only a very small minority of those surveyed believe that there is no risk at all associated with the use of Shadow Code.

The lack of insight into Shadow Code is complicated by the general lack of trust that website operators have of their business partners.

Figure 9
Level of Security Risk Posed by Running Shadow Code



Source: Osterman Research, Inc.

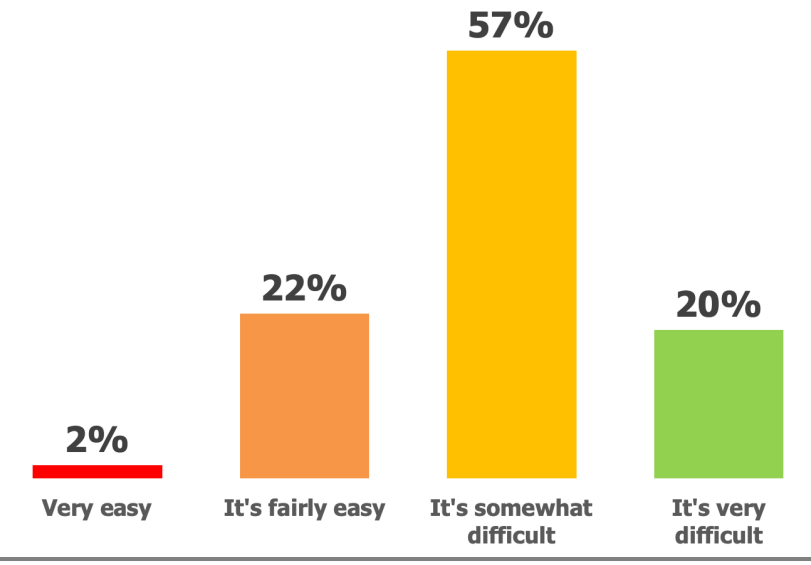
It's also noteworthy that the proportion of those who believe that Shadow Code is risky has increased year-on-year. As shown in Figure 10, 59 percent of those knowledgeable about their organizations' websites considered Shadow Code to be risky in our 2019 survey, but that has jumped to 69 percent in the current survey.

BAD ACTORS CAN EASILY ABUSE THIRD-PARTY CODE

Our research found that third-party code is perceived by website decision makers to be easy to hack or attack. As shown in Figure 10, 24 percent consider third-party code is either "very" or "fairly" easy to abuse for malicious purposes. Another 57 percent believe that third-party code is "somewhat" difficult to abuse, while only 20 percent believe that doing so is "very" difficult.

More than 69% believe that Shadow Code poses significant to serious risks.

Figure 10
Perceived Ease With Which Bad Actors Can Abuse Third-Party Code



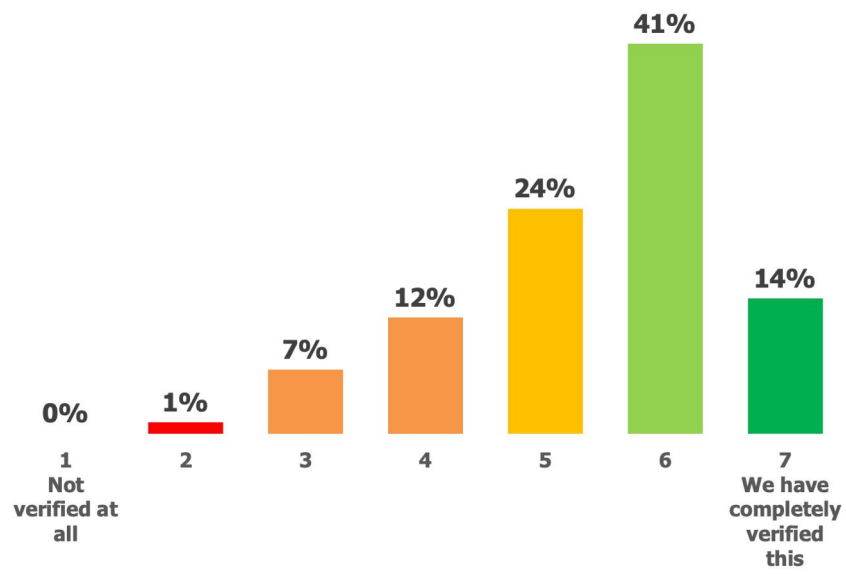
Source: Osterman Research, Inc.

The data in the figure above underscores one of the most serious problems with current website deployments: much, if not most, of the code running on the typical website consists of third-party code, and a significant proportion of it is easily hackable by malicious actors. This problem has been exacerbated by the COVID-19 pandemic that has diverted security teams' attention to other aspects of security as they were enabling their workforces to operate from home or otherwise remotely, taking their attention away from key areas – like corporate web properties – that are drawing increased attention from bad actors.

FIRST-PARTY RISKS REMAIN SIGNIFICANT

While most of those knowledgeable about their organizations' websites perceive Shadow Code from external sources to be risky, the vast majority have yet to completely verify that their internally-generated scripts are not risky, making even that code risky to operate. As shown in Figure 11, only 14 percent of organizations have "completely" verified that their internally-generated code does not pose a security risk, while another 41 percent have "mostly" verified that this is the case. The remaining 45 percent are even less sure that the internally-developed code running on their web properties is secure.

Figure 11
Extent to Which Organizations Have Verified That Internally-Generated Scripts Do Not Pose a Security Risk



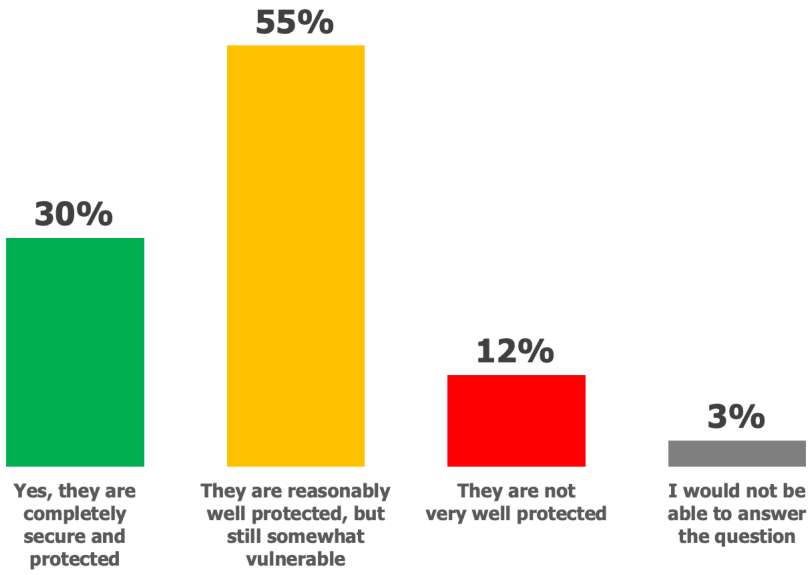
Source: Osterman Research, Inc.

The proportion of those who believe that Shadow Code is risky has increased year-on-year.

MOST ARE NOT SURE THEIR WEB PROPERTIES ARE COMPLIANT

Privacy obligations, such as those imposed by the European Union's GDPR, the CCPA, and other, similar regulations pose a number of important requirements on website operators. However, as shown in Figure 12, only 30 percent of respondents to the survey reported that their externally facing web properties are "completely secure and protected". This is down from 38 percent last year. Moreover, while 55 percent report that their web properties are "reasonably" well protected, 12 percent indicated that these properties are not at all well protected.

Figure 12
Extent to Which Decision Makers Could Confirm That Their Externally Facing Web Properties are Secure and Compliant With the GDPR, CCPA and Similar Types of Data Privacy Regulations



Source: Osterman Research, Inc.

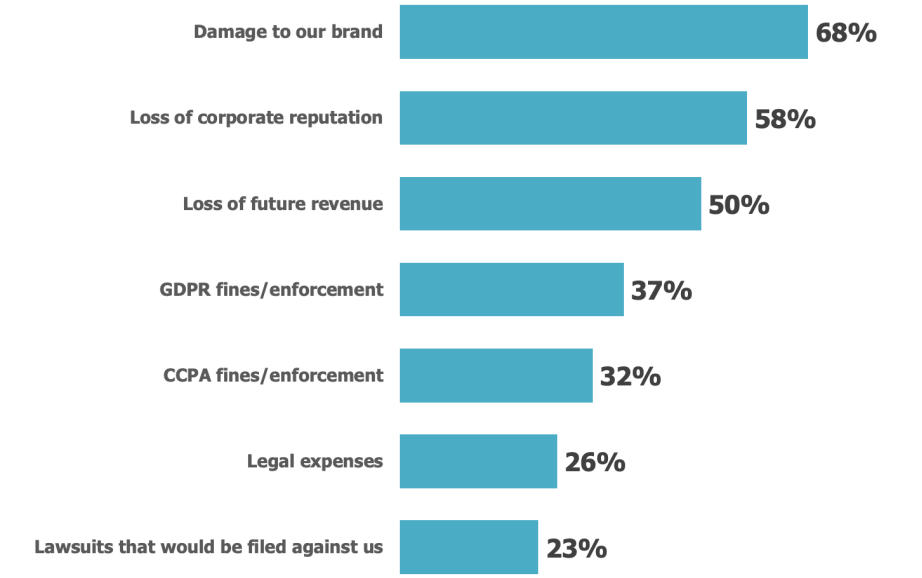
Data Breaches Have Serious Consequences

CONSEQUENCES TO THE BUSINESS

What are the consequences that an organization would suffer following a major data breach that was the result of malicious Shadow Code running on an externally-facing, corporate website? As shown in Figure 13, the consequences for most would be serious and varied. For example, 68 percent reported that a "major" or "huge" anticipated problem would be damage to their brand, 58 percent reported that the loss of corporate reputation would be this serious, and 50 percent believe that there would be loss of future revenue.

The vast majority have yet to completely verify that even their internally-generated scripts are not risky.

Figure 13
Consequences of a Major Data Breach Caused by Malicious Shadow Code in Externally-Facing Websites
Percentage responding a major or huge problem



Source: Osterman Research, Inc.

Damage to the brand was the top concern from data breaches caused by Shadow Code on external websites?

It's important to note that the consequences of a website-related data breach can vary widely by industry. For example, in addition to many of the consequences noted above, a financial services firm in the United States that experienced a data breach would likely face sanctions and other penalties from the Securities and Exchange Commission and the Financial Industry Regulatory Authority.

While most organizations cannot demonstrate compliance with privacy regulations like the GDPR or CCPA, they must be able to do so. In the case of the CCPA, for example, if an organization is responsible for the breach of non-encrypted or non-redacted information about a California consumer, there are two penalties that can apply to the company that allowed the breach to occur:

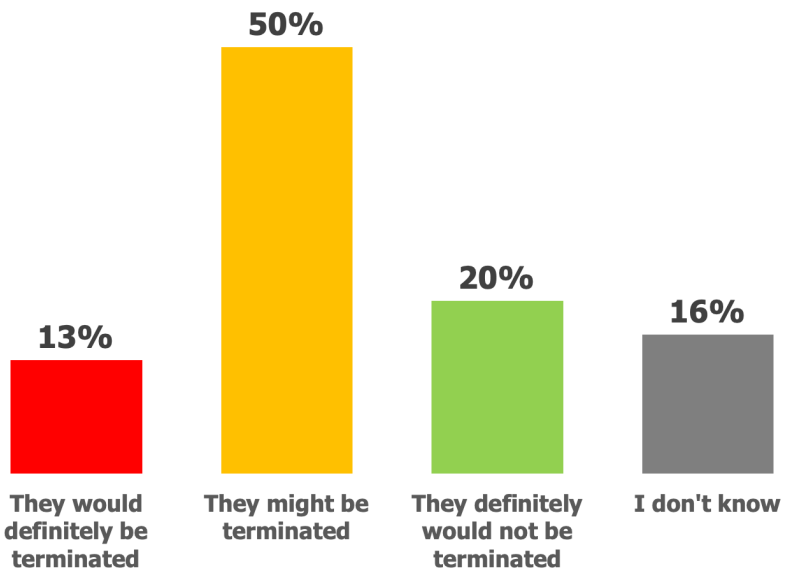
- A consumer whose data was breached may be entitled to recover damages of $100 to $750 or the actual damages from the breach, whichever is greater; injunctive or declaratory relief; or any other relief determined by a court [Section 1798.150(a)(1)(A-C)].

- The State of California Attorney General's office may also impose fines of $2,500 or $7,500, respectively, for each non-intentional or intentional violation of the CCPA.

THE PERSONAL CONSEQUENCES OF A MAJOR DATA BREACH WOULD BE SERIOUS

What would happen to those in charge of externally-facing web properties if there was a major data breach as a result of malicious Shadow Code running in them? As shown in Figure 14, 13 percent of those knowledgeable about their organization's web properties report that those in charge would "definitely" be terminated, and another 50 percent report that this might be their fate. Only 20 percent reported that those in charge would definitely not be terminated, while another 16 percent really don't know what would happen.

Figure 14
Consequences of a Major Data Breach as a Result of Malicious Shadow Code in Externally Facing Websites



Source: Osterman Research, Inc.

Interestingly, we found significantly fewer organizations in the 2020 survey reporting that security staffers would be terminated following a data breach than we found in the 2019 survey.

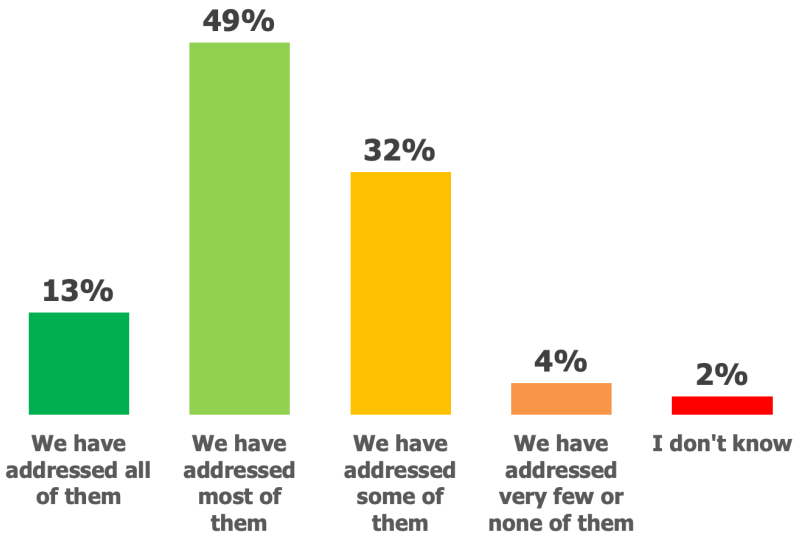
Managing the Risks from Shadow Code

THE MAJORITY HAVE ADDRESSED MOST OR ALL OF THEIR KNOWN VULNERABILITIES

Some good news that came from the survey is that known vulnerabilities in the third-party scripts running on corporate websites are being addressed. For example, as shown in Figure 15, 13 percent of those knowledgeable about their corporate web properties report that all of the known vulnerabilities have been addressed, while another 49 percent reported that most of them have been. That leaves another 38 percent of respondent organizations that have, at best, addressed only some of these vulnerabilities, while a small handful have either addressed none or very few of them.

While most organizations cannot demonstrate compliance with privacy regulations like the GDPR or CCPA, they must be able to do so.

Figure 15
Extent to Which Organizations Have Addressed Known Vulnerabilities from Third-Party Scripts



Source: Osterman Research, Inc.

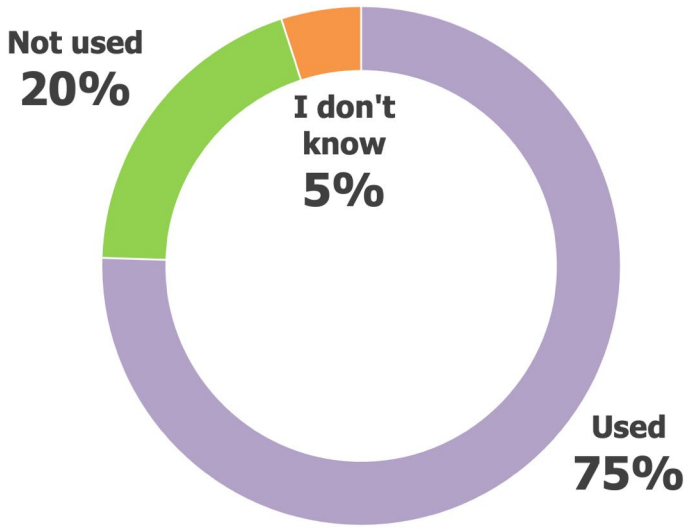
Of course, only those vulnerabilities that are known can be addressed, and it's likely that the concerted and well-funded efforts of bad actors will introduce more vulnerabilities even in code for which "all" vulnerabilities have been addressed.

Known vulnerabilities in the third-party scripts running on corporate websites are being addressed.

MOST USE CONTENT SECURITY POLICIES

Content security policies, which provide an additional layer of protection to defend against things like cross-site scripting attacks, are used by the majority of organizations to protect their websites. As shown in Figure 16, 75 percent are using content security policies, while only 20 percent are not. A small handful of respondents indicated that they don't know if these policies are in use or not.

Figure 16
Use of Content Security Policies on Corporate Websites

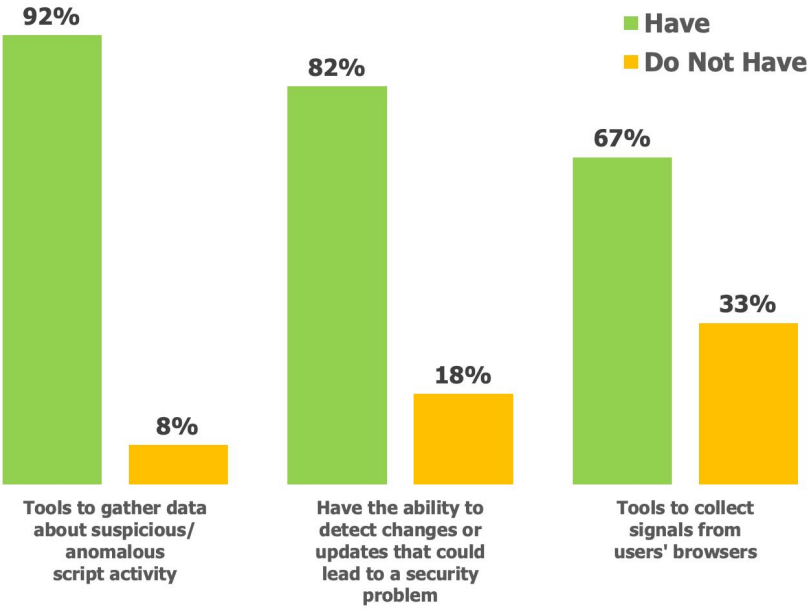


Source: Osterman Research, Inc.

PROGRESS IS BEING MADE WITH MANAGEMENT TOOLS

As shown in Figure 17, the vast majority of organizations have tools and other capabilities in place that are focused on protecting their websites from various threats. For example, 92 percent of those surveyed have tools in place that will gather data about suspicious or anomalous script activity; and 67 percent have tools to collect signals from users' web browsers, such as network activity, storage activity or Document Object Model events. Moreover, 82 percent of those surveyed indicated that their organization has the ability to detect changes or updates that could lead to a security problem.

Figure 17
Availability of Tools and Capabilities to Manage Corporate Websites



Source: Osterman Research, Inc.

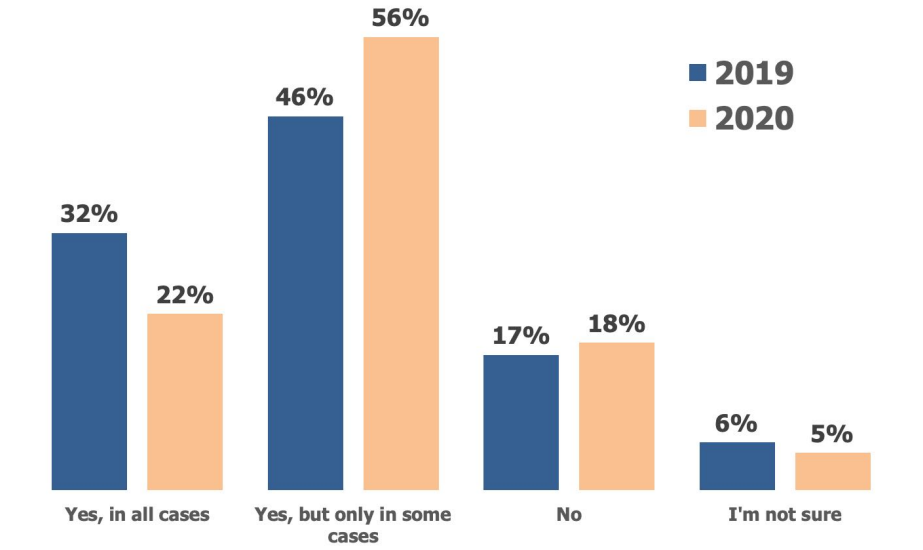
The concerted and well-funded efforts of bad actors will discover more vulnerabilities even in code for which "all" vulnerabilities have been addressed.

Our research also found that the proportion of organizations that have deployed these capabilities is increasing. For example, while 92 percent today have tools in place to detect suspicious or anomalous activity, this figure was 89 percent in the 2019 survey. Those organizations that have the ability to detect changes or updates that could lead to a security problem has jumped to 82 percent in 2020 from just 61 percent in 2019. Organizations with tools to collect users' browser signals has edged up slightly, from 65 percent in 2019 to 67 percent in 2020. All of this indicates progress is being made in understanding web-based threats and, specifically, those inherent in much third-party code.

LIMITED OPTIONS TO CONTROL SHADOW CODE

Shutting down suspicious scripts and those that exhibit anomalous behavior is an essential element in preventing malicious behavior, data breaches, and the like on corporate websites. However, as shown in Figure 18, most organizations do not give their security teams the authority to exercise this capability and the proportion that do is falling. While 32 percent of security teams in the 2019 survey could shut down websites displaying anomalous behavior, this has dropped to 22 percent this year. The proportion of security teams that cannot shut down websites has remained virtually constant year-on-year.

Figure 18
Extent to Which the Security Team Responsible for Externally-Facing Websites Has the Authority to Shut Down Suspicious Scripts



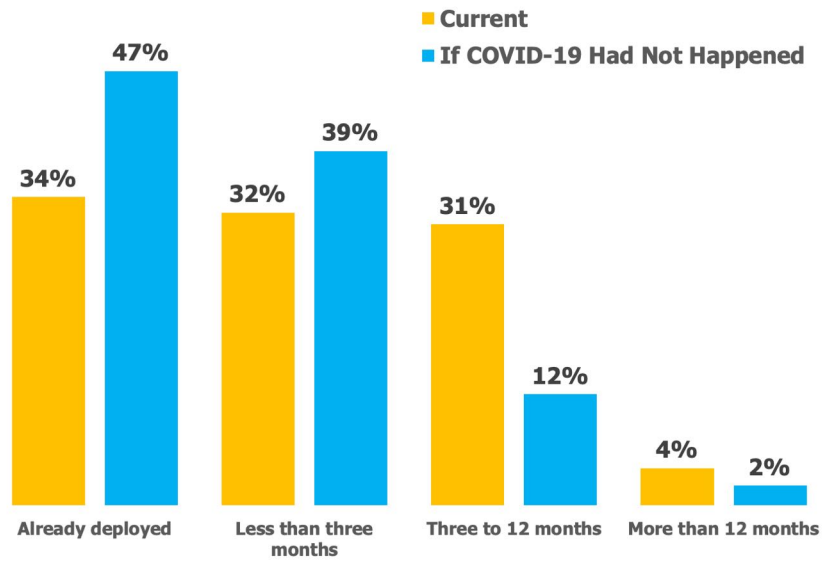
Source: Osterman Research, Inc.

COVID-19 HAS SLOWED ADOPTION OF SHADOW CODE MANAGEMENT SOLUTIONS

The COVID-19 pandemic has had significant and far-reaching impacts on virtually every aspect of life, and its impact has also been felt on web security. When those knowledgeable about how their websites operate were asked about the anticipated timeframe for deploying web security solutions, they reported that deployment of these solutions has been significantly delayed. For example, as shown in Figure 19, 34 percent have already deployed some sort of web security solution, while another 32 percent planned to do so in the three months following the survey. However, had the COVID-19 pandemic, along with government-imposed lockdowns and other economic impacts not occurred, these figures would have been 47 percent and 39, respectively. In other words, while 66 percent of organizations have already deployed some type of web security solution or planned to do so in the very near term, this would have been 86 percent in the absence of the COVID-19 pandemic.

Shutting down suspicious scripts and those that exhibit anomalous behavior is an essential element in preventing malicious behavior.

Figure 19
Currently Anticipated Timeframe for Deploying Solutions to Address Shadow Code Compared to Timeframe if the COVID-219 Pandemic Had Not Occurred



Source: Osterman Research, Inc.

Summary

Modern websites and applications will continue to leverage third-party scripts and libraries to innovate faster. This Shadow Code can introduce unknown security risks into an organization, including malicious scripts that can skim user data and lead to client-side data breaches and compliance penalties. However, while many organizations are improving their ability to address the problems inherent in Shadow Code by deploying the appropriate technologies and vetting third-party sources, trust in the digital supply chain remains low. Organizations must balance the agility provided by third-party scripts and libraries with effective visibility and security controls to ensure they can reduce the risk of data breaches and comply with regulations.

About PerimeterX

PerimeterX is the leading provider of application security solutions that keep digital businesses safe. Delivered as a service, the company's Bot Defender, Code Defender and Page Defender solutions detect risks to web applications and proactively manage them, freeing companies 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.

While 66 percent of organizations have already deployed some type of web security solution or planned to do so…this would have been 86 percent in the absence of the COVID-19 pandemic.