Sectigo State of Website Security and Threat Report

PUBLISHED 2021

SECTIGO®

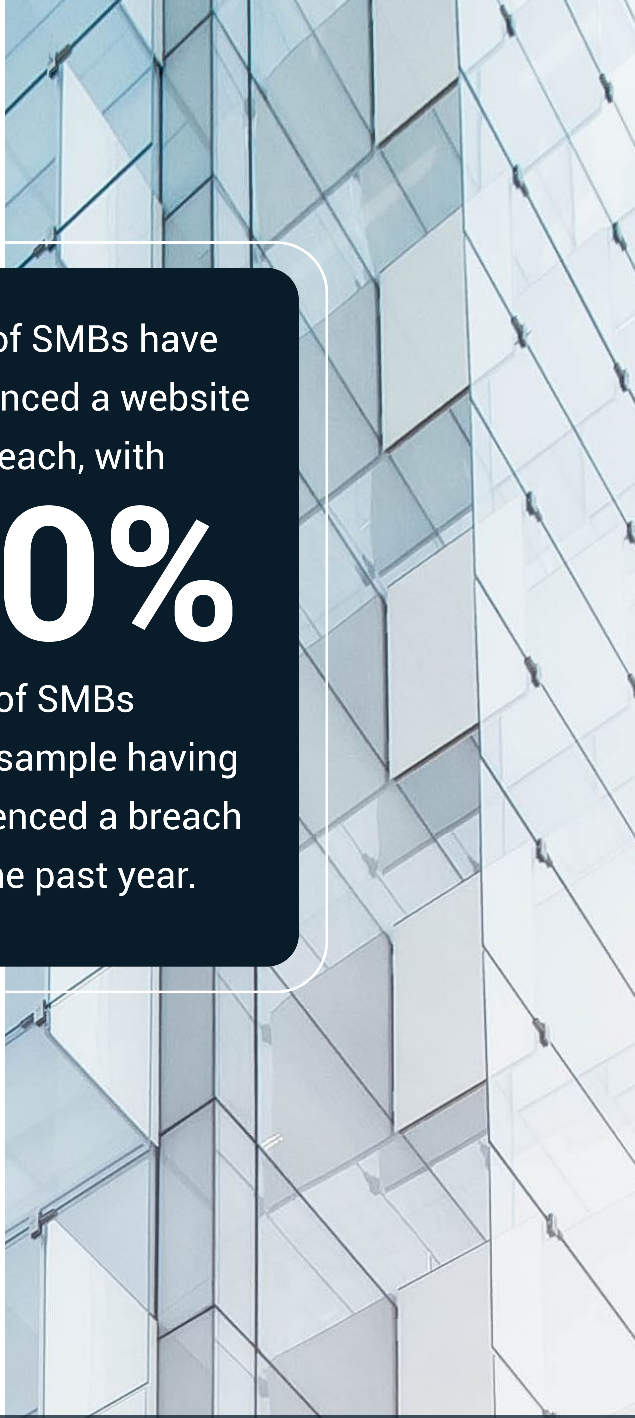
Executive Summary

Website security is not top of mind for most small- to medium-sized businesses (SMBs). Their focus is understandably on getting products and services to market, managing their core operations, and serving the needs of their customers, particularly during the pandemic. And most SMBs lack the in-house security personnel and skills required to address website security.

But lack of attention does not equate to lack of importance. Website security is critical, regardless of your business' size. As businesses digitize their operations, their websites are becoming increasingly mission-critical for both business operations and customer communication. Alarmingly, these same websites are also a growing conduit for risk.

Sectigo recently conducted a survey of SMBs to better understand the role websites play in each business, the degree of risk these sites represent, and how prepared SMBs are to secure them. According to our study, SMBs are confident in their website security stance; in fact, they appear to be overconfident. Forty-eight percent believe they are too small to be attacked, and 75% believe they are effectively mitigating website risks.

But our study also showed that the reality is much different. SMBs feel they are safe...until it's too late. SMBs' websites are under constant risk of attack, with half having experienced a website breach at some point in the past, and 20% of the sample having experienced a breach within the last 12 months. And the cost of breaches is high, with the top impacts being website outage or downtime, loss of time/employee productivity, and loss of customer confidence/reputation.



Half of SMBs have experienced a website breach, with

20%

of SMBs
in our sample having experienced a breach in the past year.

Considering how important website security is to their businesses, SMBs are spending relatively little on it, with 60% spending $500 or less per month. However, 49% of SMBs are planning to spend more in 2021, with the realization that 2021 is likely to bring more sophisticated and more frequent attacks.

To prepare themselves for today's threat landscape, SMBs need to align themselves with a security provider that can provide holistic, all-in-one solutions. They need a partner with the resources to stay on top of the evolving security/threat landscape so the SMB doesn't have to. They need a solution that they can "set and forget" so they can focus on their core businesses. They also need to understand that security is a journey, not a destination. Simply putting a static solution in place will not suffice. Today's SMBs need an automated solution from a trusted security leader dedicated to constantly adapting and adjusting the solution to guard against evolving security threats. This will enable SMBs to enjoy peace of mind while continuing to focus on what they do best.

About This Study

This report is based on a global, web-based survey of 1,167 website security decision makers at SMBs with 500 employees or less. Organizations were headquartered in 9 countries: Australia, Brazil, China, France, Germany, India, Mexico, the United Kingdom, and the United States. Organizations represented a range of industries, with a primary emphasis on technology, retail, and financial services. The survey was conducted in November 2020.

49%

of SMBs are planning to spend more on website security in 2021.

SMBs Are Confident They Aren't Vulnerable…
Yet Many Have Experienced High-Impact Breaches

Generally speaking, SMBs don't believe they are terribly vulnerable to online threats, with only 31% stating that they feel vulnerable or very vulnerable (Figure 1). As this report will show, this confidence represents a blind spot for many SMBs, who are actually substantially more vulnerable than they think. Interestingly, those who have experienced breaches in the past 12 months have a much more realistic assessment of their vulnerability, with 58% feeling vulnerable or very vulnerable.

SMBs Believe Their Websites Is Vulnerable to Online Threats

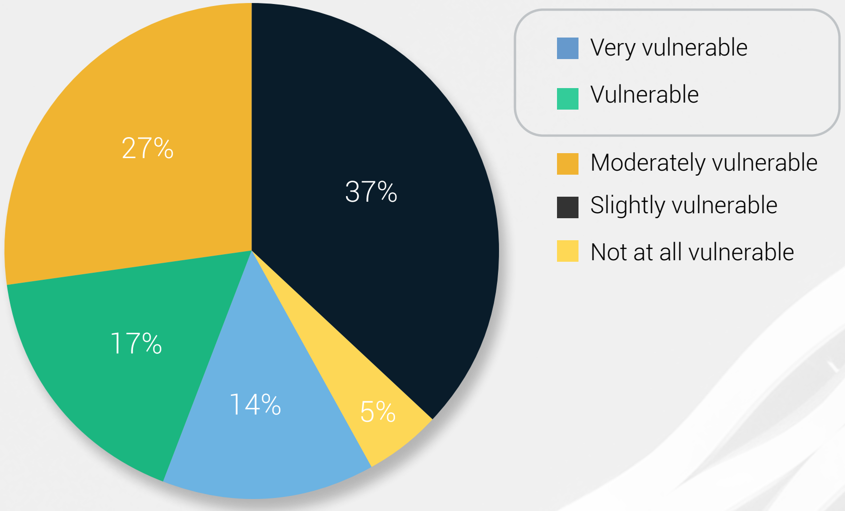


Figure 1

n = 1,167
Source: State of Website Security and Threat Report, January 2021

48% of SMBs say they are too small to be a target of cyberattacks

SMBs Believe They Are Effectively Mitigating Risks

The lack of feelings of vulnerability may spring from SMBs' confidence in their website security stance, with 73% saying they agree or strongly agree that they are effectively mitigating risks, vulnerabilities, and attacks to their website (Figure 2). Another contributing factor is that many feel they are just not a focus for attackers, with 48% saying they are too small to be targets of cyberattacks.

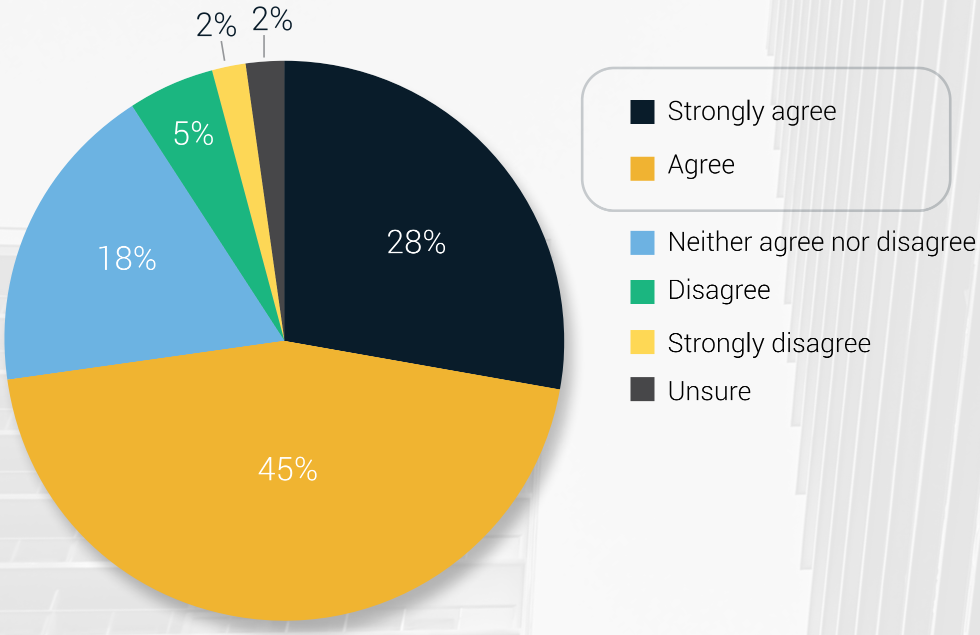


Figure 2

n = 1,167
Source: State of Website Security and Threat Report, January 2021

54% say there would be a serious impact to their business if their website went down.

SMBs with Websites Breached by an Attack

And yet, websites represent a significant point of vulnerability. Fifty-four percent of SMBs say there would be a serious impact to their business if their website went down, and 72% say they collect or store sensitive data through their website.

Website breaches are far too common. Half of SMBs have experienced a website breach, and 20% of our sample experienced one just in the past 12 months (Figure 3). And these are the ones who even know they were breached; the actual numbers are likely significantly higher. Reported breaches are even higher for companies in the financial services industry, 52% of whom say that their website has been breached in the past year, and in China, where 66% of SMBs report that their website has been breached in the past year. Interestingly, only 9% of UK SMBs reported a breach in the past 12 months.

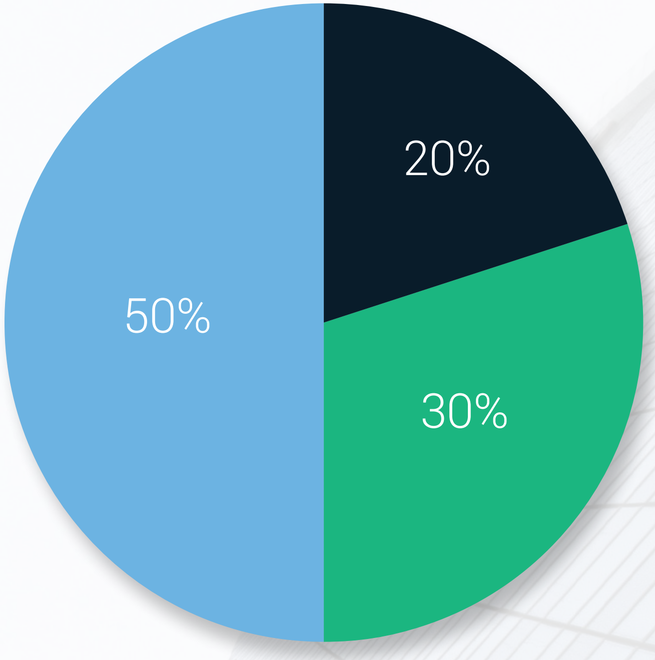


Figure 3

n = 1,167
Source: State of Website Security and Threat Report, January 2021

Severity of Website Breach Impact

And the cost of these breaches is high. Twenty-eight percent of those who had been breached said the consequences were severe or very severe (Figure 4). This figure grows to 40% of financial services respondents whose site has been breached and 41% of Chinese respondents whose site has been breached. Only 5% of UK respondents who were breached considered it "severe" or "very severe."

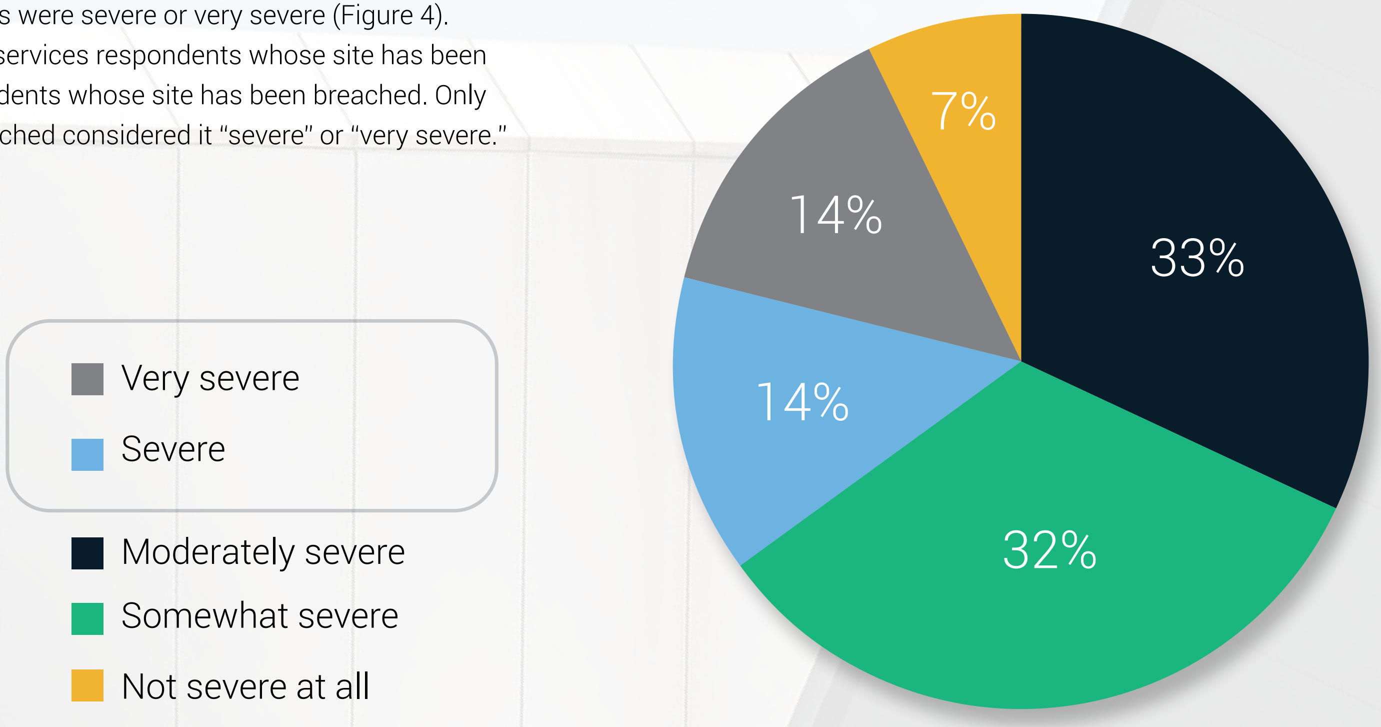


Figure 4

n = 582
Source: State of Website Security and Threat Report, January 2021

Consequences of Website Breaches

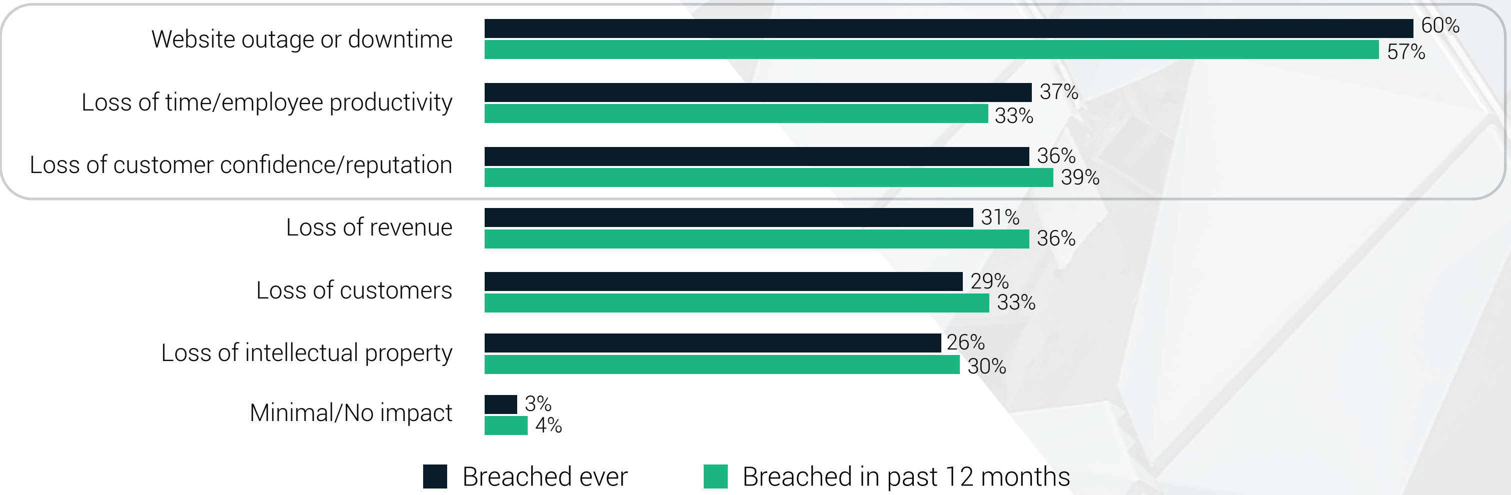


Figure 5

n = 582
Source: State of Website Security and Threat Report, January 2021

Of those that experienced a breach, the top impacts were website outage or downtime, loss of time/employee productivity, and loss of customer confidence/reputation (Figure 5). Only 3% of businesses who were breached said there was no impact, and the number of businesses where breaches led to revenue loss was about ten times that number.

Financial services respondents who experienced a breach were much more likely to report loss of revenue (40%) and loss of intellectual property (37%). And for far too many SMBs, the decision to implement website security comes too late: for 63% of SMBs that experienced a breach, that breach occurred before they implemented their website security.

Only 3% of businesses who were breached said there was no impact, and the number of businesses where breaches led to revenue loss was about ten times that number.

Vulnerability to Website Security Threats

When asked what website threats SMBs consider potential vulnerabilities, data breaches and malware injection attacks lead the list, although responses did span a range of threat vectors (Figure 6). Adding to the theme that breaches sharpen awareness of their vulnerability, SMBs who have not been breached feel less vulnerable to data breaches (23%) than those who have ever been breached (51% of those who have ever been breached feel vulnerable, as do 61% of those breached in the last 12 months).

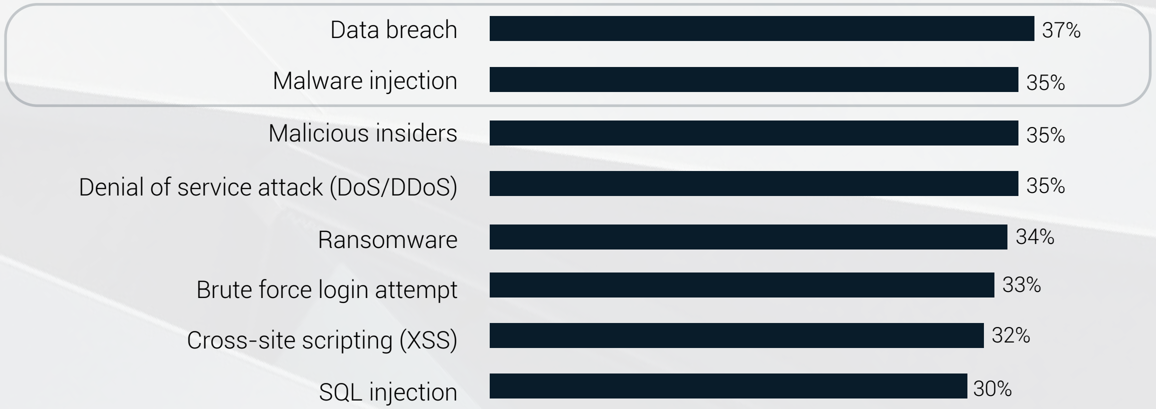


Figure 6

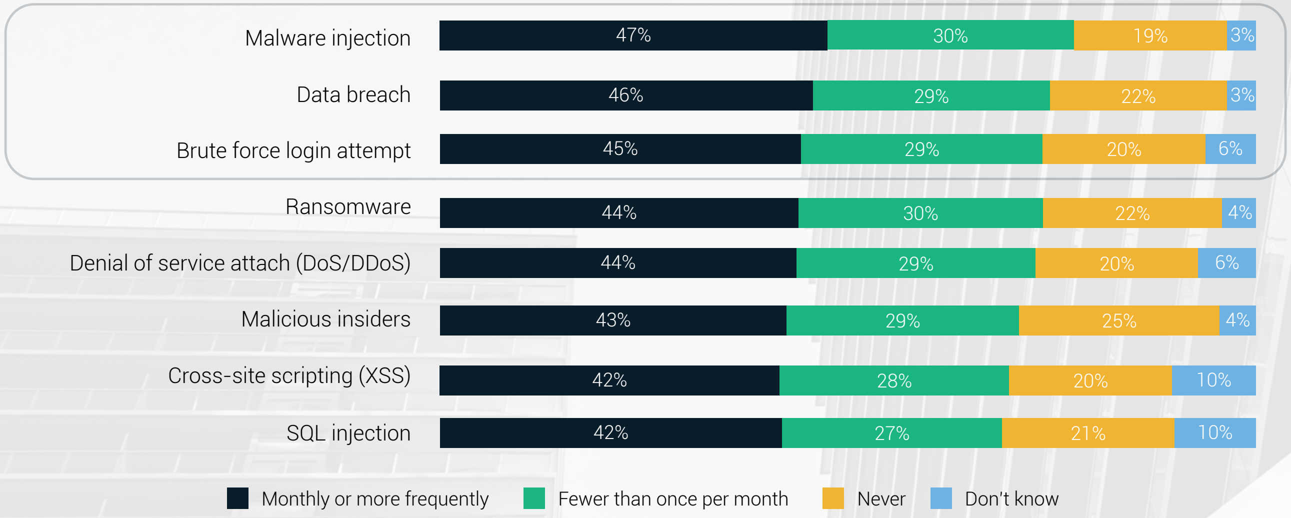
n = 1,167; top-2 box analysis
Source: State of Website Security and Threat Report, January 2021

For **63%** of SMBs that experienced a breach, that breach occurred before they implemented their website security.

SMBs Face Constant Attacks from Many Threat Vectors

SMBs are under constant attack. More than 40% of SMBs report a broad range of attacks targeting their websites on a monthly or more frequent basis, with malware injection, data breach threats, and brute force login attempts leading the list (Figure 7). Thirty percent of Chinese SMBs say they face data breach threats daily or more frequently. Seventy-five percent of the global sample say that they have been subject to a malicious insider at some point in the past. And these are the attacks that they are aware of.

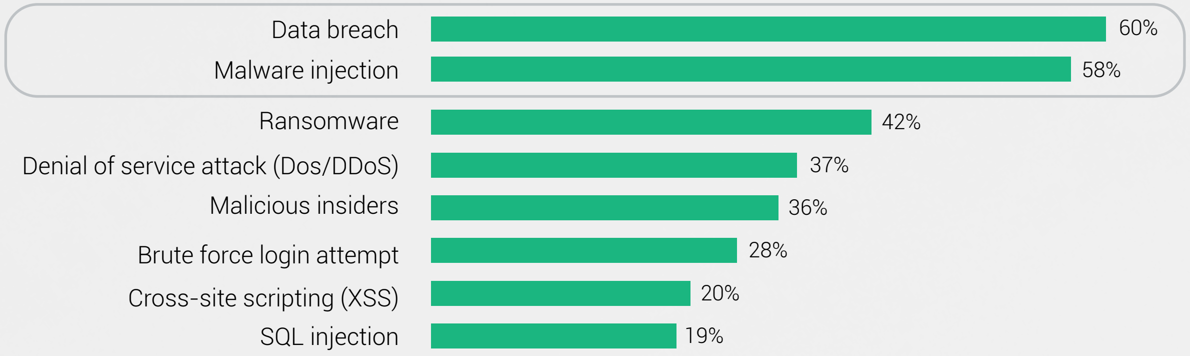
Figure 7 – Frequency of Website Security Threats



n = 1,167
Source: State of Website Security and Threat Report, January 2021

More than **40%** of SMBs report a broad range of attacks happening to their website on a monthly or more frequent basis.

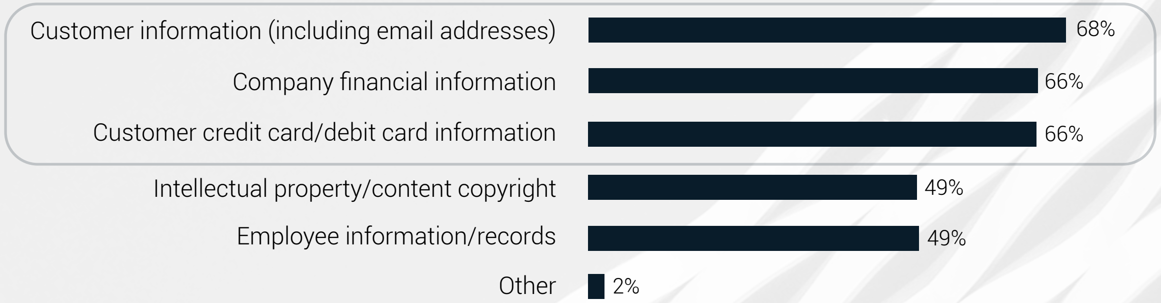
Figure 8 – Website Security Threats of Greatest Concern



n = 1,167
Source: State of Website Security and Threat Report, January 2021

And while they feel vulnerable to a wide range of threats (from Figure 6), there was a great deal more stratification when asked which they are more concerned about (Figure 8). Data breaches and malware injection again lead the list with 60% and 58% ranking them as concerns, respectively. But now brute force logins, cross-site scripting, and SQL injection fall much lower down with 28% or fewer listing them as concerns. This is evidence of SMBs' blind spots as these are some of the threats that cause the greatest harm for websites, while data breaches and malware injection actually represent a lower risk.

Figure 9 – Information Most Concerned with Protecting



n = 1,167
Source: State of Website Security and Threat Report, January 2021

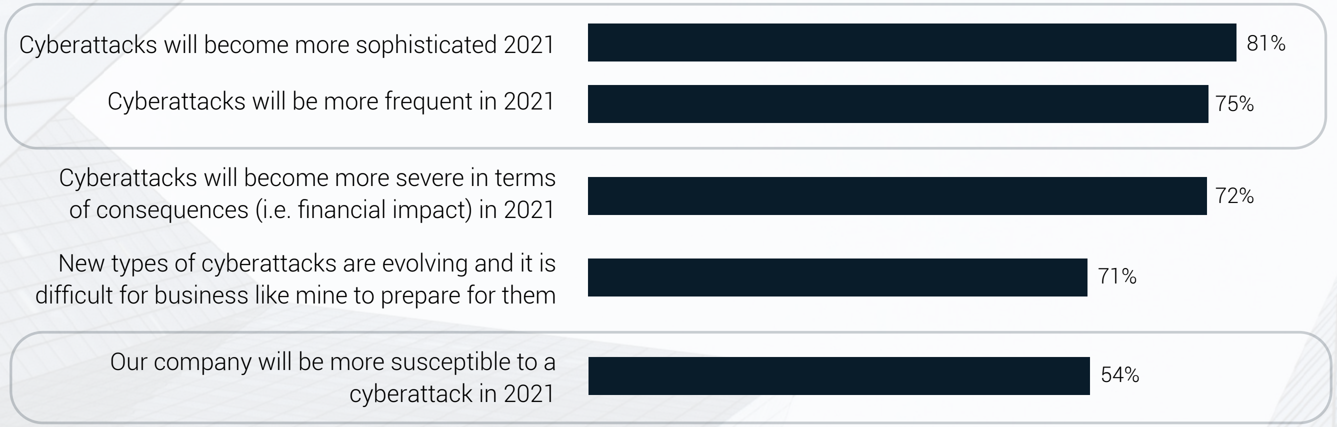
The information respondents are most concerned about protecting includes customer information, company financial information, and customer credit card information (Figure 9). Retail businesses are, not surprisingly, most concerned about protecting customer credit card information (76%) and customer information (74%).

SMBs Look to Increase Security Stance in 2021

SMBs see more frequent and more sophisticated website attacks in store for 2021. Eighty-one percent believe cyberattacks will become more sophisticated, and 75% believe they will become more frequent in 2021 (Figure 10). Seventy-one percent believe that it is difficult for SMBs to prepare for the growing sophistication of attacks, yet only 54% believe they themselves will be more susceptible to a cyberattack. This again points to the disconnect between security reality and respondents' overconfidence in their ability to repel an attack and could be indicative that while SMBs understand that cyberthreats are significant in theory, no one expects one to happen to them.

While SMBs understand that cyberthreats are significant in theory, no one expects one to happen to them.

Figure 10 – 2021 Website Security Outlook



n = 1,167; top-2 box analysis
Source: State of Website Security and Threat Report, January 2021

Figure 11 – Monthly Website Security Budget

Considering how important SMBs' websites are, they are spending relatively little to secure them. Sixty percent of SMBs spend $500 per month or less for website security (Figure 11), which is closely consistent for both SMBs that have experienced a breach in the past year and those that have not. Average website security spending across the sample is $461.[1]

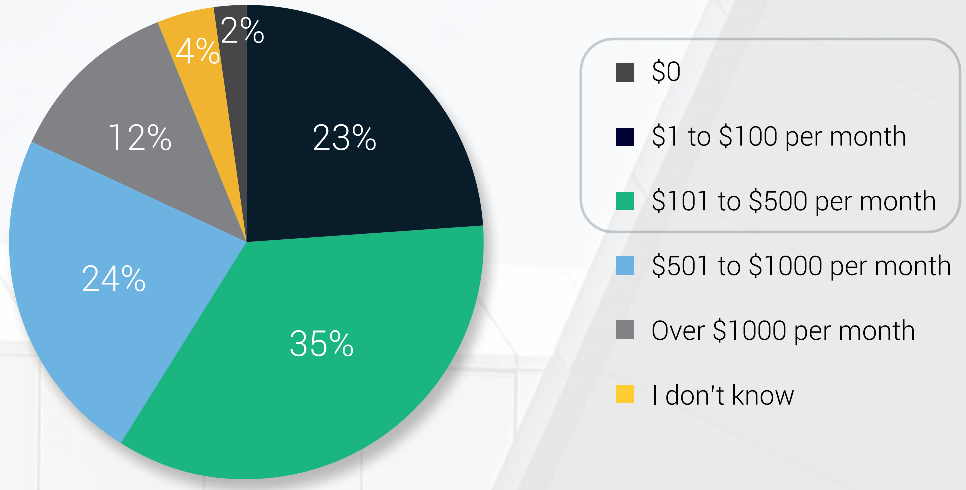


Figure 11

n = 1,167

Source: State of Website Security and Threat Report, January 2021

Figure 12 – Planned Website Security Spending in 2021

Forty-nine percent of respondents are increasing their website security spending in 2021, and only 1% plan to decrease it (Figure 12). Financial services companies are leading the charge, with 69% planning to increase website security spending in 2021, followed by companies in technology (62%) and retail (52%).

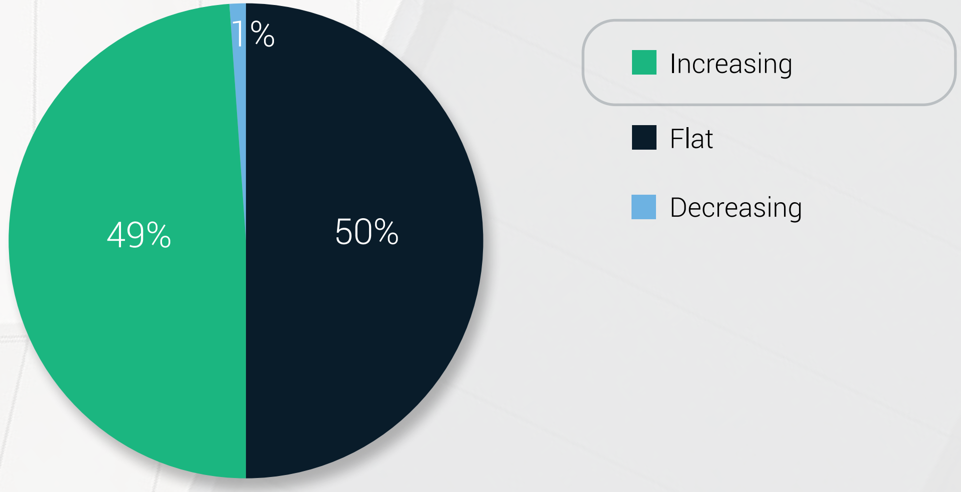


Figure 12

n = 1,167

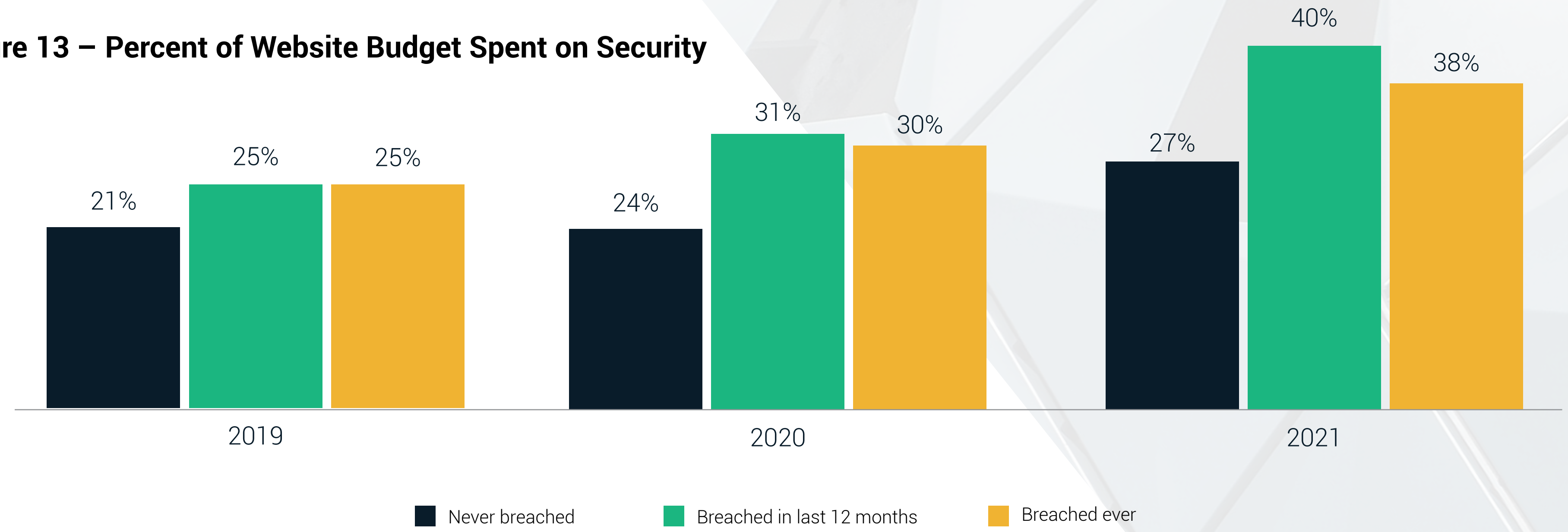
Source: State of Website Security and Threat Report, January 2021

[1] Average website spending estimates based on midpoint analysis calculations on budget ranges contained in survey. Global percentages are an average of the entire sample, derived from approximately equivalent ranges based on November 2020 currency conversions (rounded to respondent-friendly currency breaks).

SMBs that have experienced a website breach are much more likely to plan greater spending on web security in 2021 (Figure 13). Seventy-four percent of SMBs that have experienced a website breach in the last year are increasing website security spending in 2021. SMBs that feel they are not at all vulnerable to website attacks tend to spend in line with the total average (26% in 2019, 29% in 2020, 35% in 2021). But those that feel very vulnerable are allocating a significant portion of their website budget to security (31% in 2019, 36% in 2020, 47% in 2021).

n = 1,167
Source: State of Website Security and Threat Report, January 2021

Figure 13 – Percent of Website Budget Spent on Security



SMBs Rely on a Broad Set of Website Security Solutions

Ninety-four percent of respondents use security products or services to protect their website, and 93% of have some or a lot of confidence in those security products or services (Figure 14). This number dips for SMBs that have experienced a website breach in the past 12 months, with only 82% having confidence in the website security products they use. In contrast, 98% of those that have not been breached are confident in their website security Products or Services.

Confidence in Web Security Products/Services

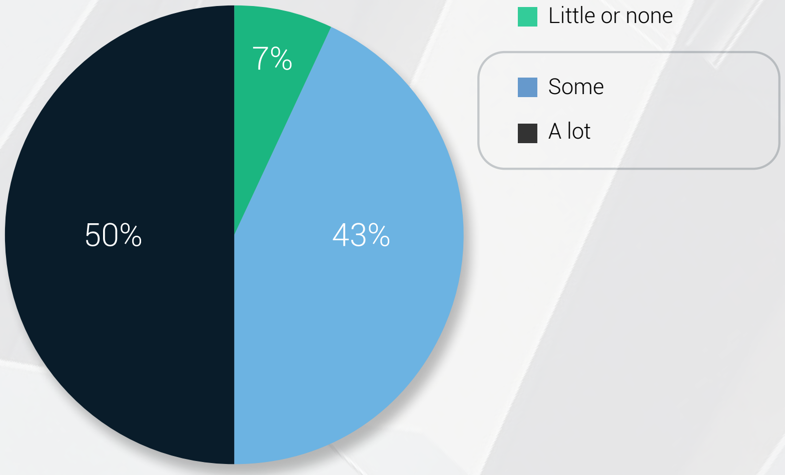
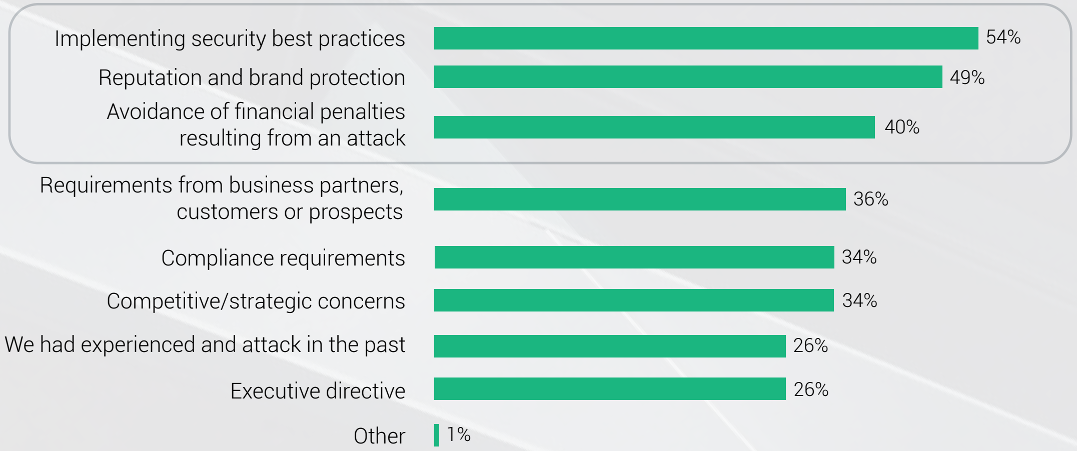


Figure 14

Figure 15 – Factors Influencing Website Security Spending



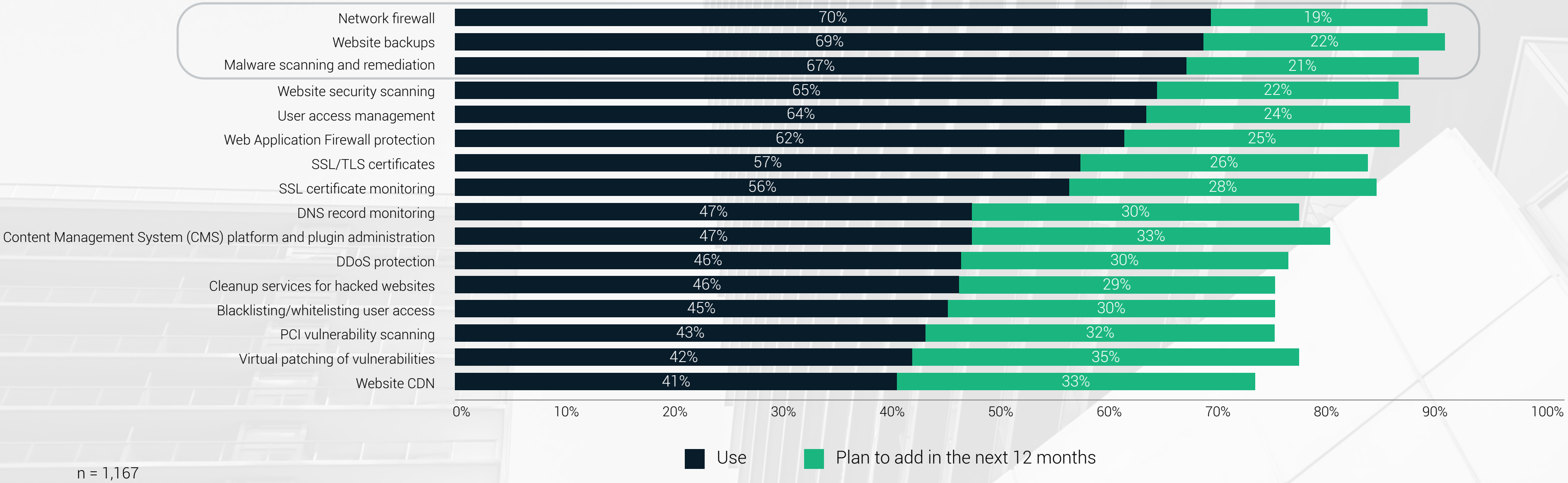
n = 1,167
Source: State of Website Security and Threat Report, January 2021

Implementing security best practices, brand protection, and avoidance of financial penalties are the most important factors influencing SMBs' security spending (Figure 15). Only 26% say that a past attack influences their website security spend.

SMBs Rely on a Broad Range of Security Technologies

Network firewalls, website backups, and malware scanning are the top website security technologies SMBs use to protect their websites (Figure 16). Businesses need all of these solutions orchestrated together to maintain a comprehensive security stance. Piecemealing a few technologies together doesn't provide proper protection as all it takes is one successful attack to inflict damage, and a patchwork of disparate types of protection can leave cracks and vulnerabilities that can be exploited by bad actors.

Figure 16 – Use of Website Security Technologies



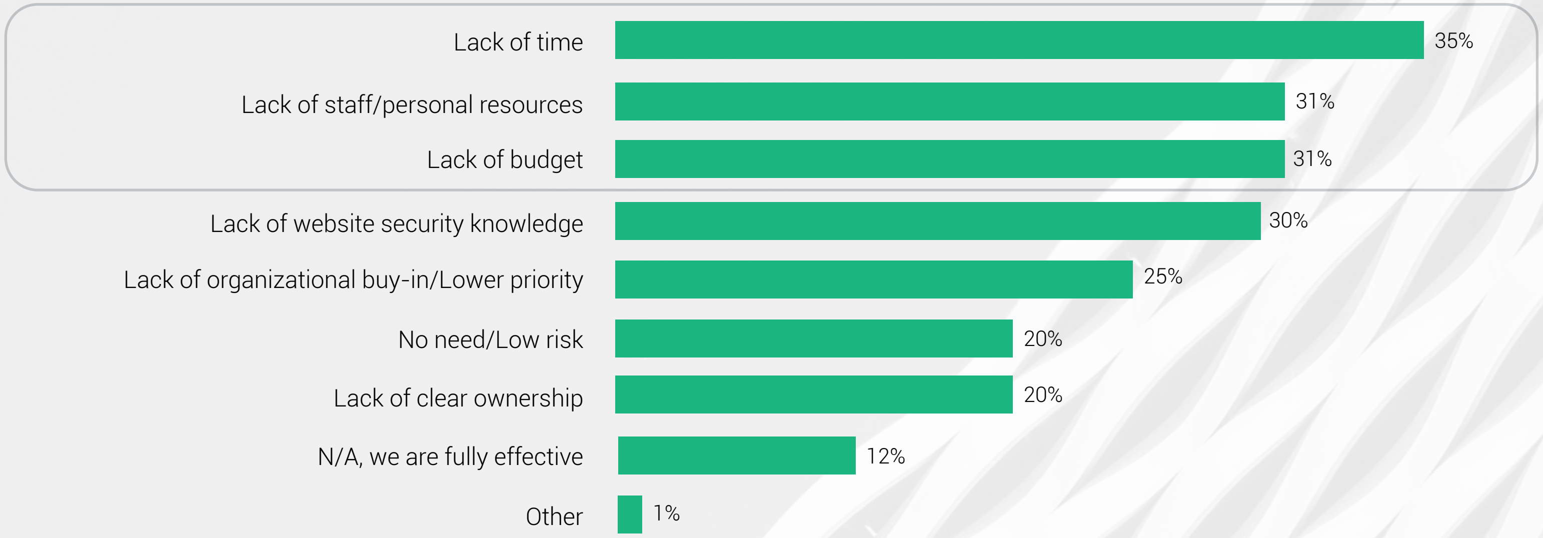
n = 1,167
Source: State of Website Security and Threat Report, January 2021

SMBs that have experienced a breach in the past 12 months use a similar mix of technologies as the general pool of respondents. By industry, technology companies currently use all of the technologies at a higher rate than respondents as a whole, while security technology usage among retail SMBs was consistently slightly lower (with the exception of PCI scanning).

SMBs Need Website Security Solutions to Be Simple and Effective

The top challenges that SMBs believe keep them from being fully effective at mitigating website risks include lack of time, resources, and budget (Figure 17). Only 12% feel they are fully effective. This speaks to one of the core issues faced by SMBs. With limited budget, resources, and personnel, SMBs require website security solutions that are easy to deploy and administer.

Figure 17 – Barriers to Use of Website Security Technologies



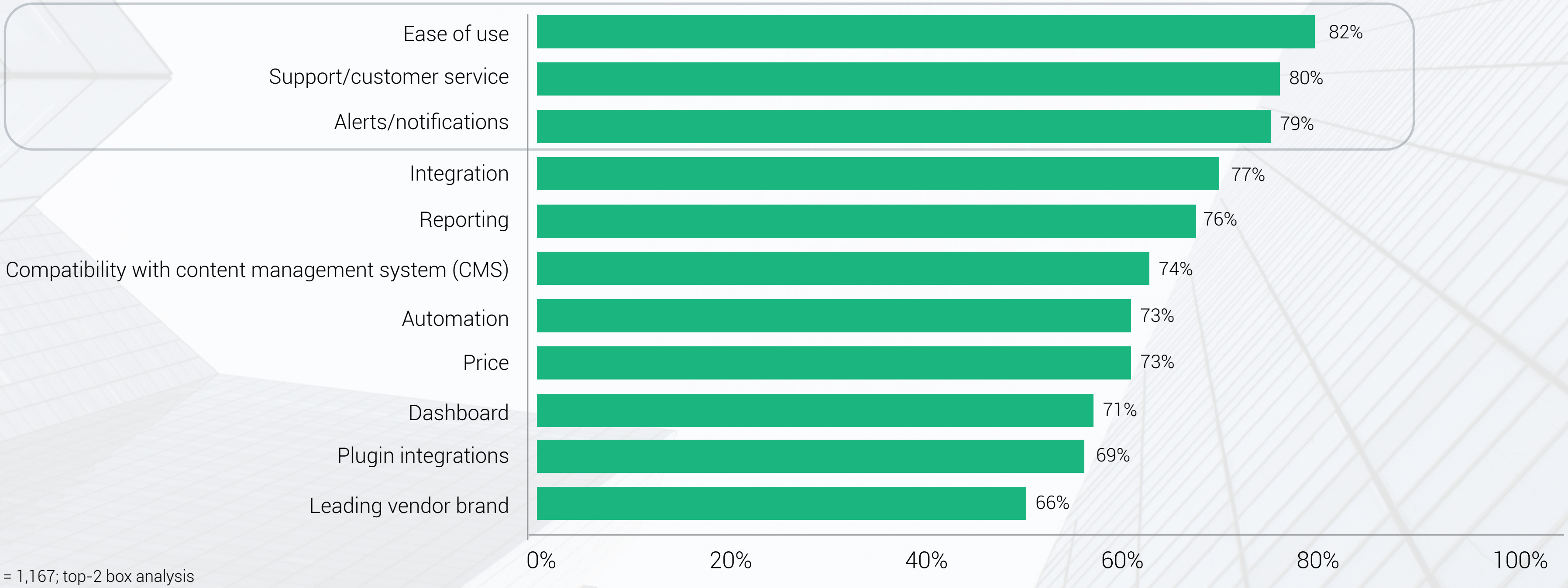
n = 1,167

Source: State of Website Security and Threat Report, January 2021

SMBs Require Easy Deployment and Administration

This point is further borne out when SMBs were asked which aspects of a website security solution are of most importance to them. Ease of use (82%), customer service (80%), and notifications (79%) lead the list (Figure 18). This speaks to their desire to have something that is easy to use, deploy, and administer. Interestingly, price is relatively low as a consideration factor, indicating that it's more important for SMBs to get something that solves their security needs than to pay the lowest possible price. Solutions must also be effective. SMBs feel their website security solution is most effective for compliance requirements (82%) and prevention of attack (80%).

Figure 18 – Importance of Website Security Aspects



n = 1,167; top-2 box analysis
Source: State of Website Security and Threat Report, January 2021

Importance of Website Security Aspect

Seventy-six percent of SMBs say they review their overall website security weekly or even more frequently (Figure 19). SMBs rely on scheduled scans (70%) and alerts (60%) to check for attacks on their website. While it's good that so many are taking an active role in their website security, it's important to be careful as there can be hidden things going on in the background of your website, and security reports are only as good as the underlying security technology. Even reviewing frequent reports, it's possible to be oblivious to malware activity that doesn't impact observable aspects of your website.

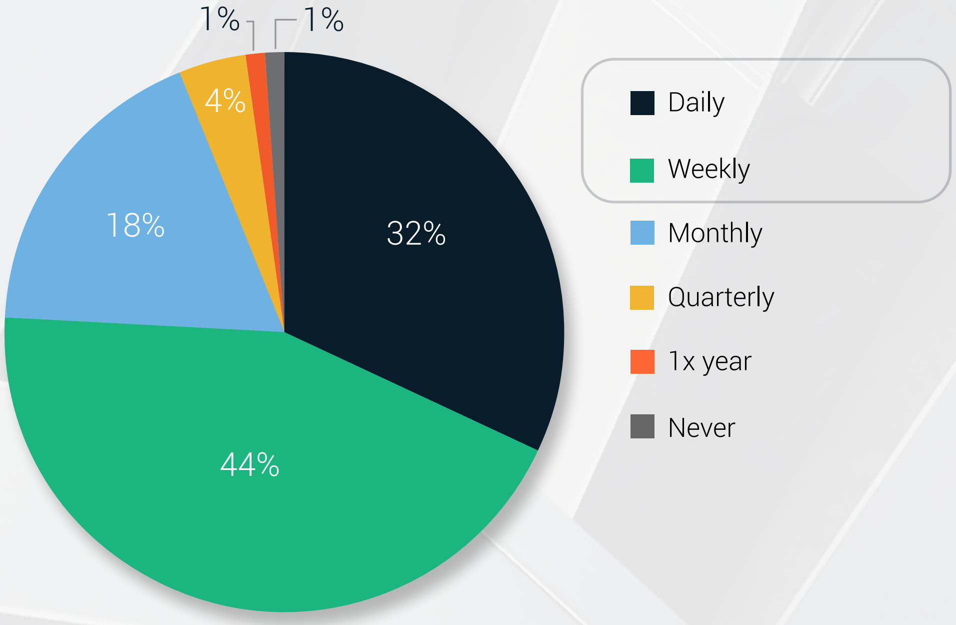


Figure 19

n = 1,167
Source: State of Website Security and Threat Report, January 2021

Key Takeaways/Guidance

This study uncovered a number of key takeaways that SMBs should consider when evaluating their website security:

- **SMBs are more vulnerable than they think.** Most SMBs believe their website is not particularly vulnerable, in part because many consider themselves too small to be a target. But this study shows that SMBs are attacked more frequently, and more damage is caused by those attacks, than is commonly believed.

- **SMBs need to stay on top of industry best practices.** Even though website security may not be top of mind for them, it is something that small/medium businesses should take very seriously. They should continually review and implement best practices that their peers and industry leaders are adopting and putting into place.

- **SMBs should look to partnerships, and not try to do it alone.** One excellent strategy is to partner with a leading website security provider that focuses on providing security solutions tailored to the needs of SMBs. This gives them the best of both worlds, allowing them to take advantage of both the depth of expertise and ability to stay up to date on security threats that a leading vendor provides while fitting within the comparatively limited budget and skill profile of most SMBs.

- **SMB web security cannot be one dimensional.** Threats are multidimensional, and SMBs expect them to get more diverse and consequential in 2021. The best approach to security is a layered, multidimensional approach that includes scanning, cleaning, monitoring, firewall, reporting, and other critical security aspects, and is designed to address the multitude of threat vectors SMBs face.

- **SMBs require a holistic, end-to-end approach in a single solution.** Piecing together separate solutions from multiple vendors across the web security technologies needed to provide comprehensive security is not only time-consuming, but is also challenging to implement and manage on an ongoing basis, particularly for SMBs with limited in-house security resources. Worse, a patchwork approach to adopting multiple vendors means that the systems are not truly working together in a seamless manner, leading to potential security gaps that can expose your website to attack.

- **SMBs need automated solutions that require minimal attention to set up and maintain.** SMBs are busy running their businesses and lack IT security departments that can provide ongoing, hands-on management of their security tools and infrastructure. They need tools that they can set and forget but that still provide the highest levels of protection and the peace of mind that comes with it.

- **Security is a journey, not a destination.** It is impossible to be "100% safe" and SMBs need to invest in solutions and partnerships that will grow and evolve as threats and attack vectors evolve. Maintaining an up-to-date security stance is a continuous effort and SMBs need a partner capable of providing that level of support.

About Sectigo

Sectigo is a leading cybersecurity provider of digital identity solutions, including TLS / SSL certificates, DevOps, IoT, and enterprise-grade PKI management, as well as multi-layered web security. As the world's largest commercial Certificate Authority with more than 700,000 customers and over 20 years of experience in online trust, Sectigo partners with organizations of all sizes to deliver automated public and private PKI solutions for securing webservers, user access, connected devices, and applications. Recognized for its award-winning innovation and best-in-class global customer support, Sectigo has the proven performance needed to secure the digital landscape of today and tomorrow. For more information, visit www.sectigo.com and follow @SectigoHQ.