Web Pro Security Survey 2020

How agencies approach website security and protect their clients' websites.

Table of Contents

Web Pro Security Survey

For professionals who help clients establish a presence online, the subject of website security often flies under the radar. It's a specific niche and one that many web professionals often avoid.

To cast light on the subject, this year we look at insights from more than 200 web professionals — including web designers, developers, freelancers, and marketing agencies.

Their answers produced statistics related to:

- **Choosing service providers**
- **Approaches to website security**
- **Service offerings and tools**
- **Planning for hacks and attacks**

Each year, Sucuri produces that Web Professional Security Survey to better understand how agencies run their businesses and the challenges they face with security. This report uses data collected in 2020.

Overview

The term “web professional” loosely refers to individuals and organizations that provide services online, including:

- **Website developers and designers**
- **Marketing agencies and SEO**
- **Brand reputation agencies**
- **Web hosting providers**
- **Freelancers**
- **Managed service providers (MSPs)**

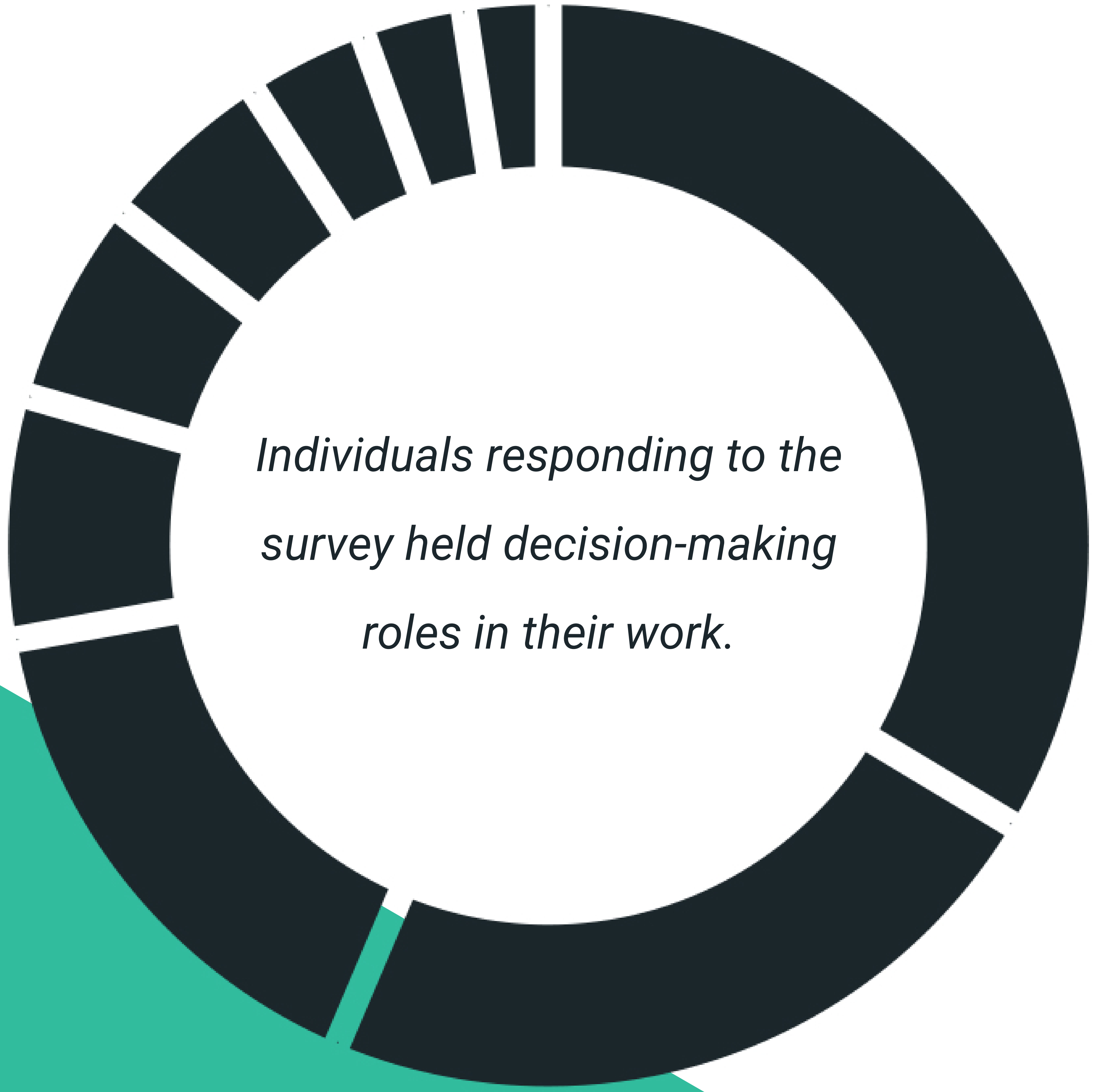
A Closer Look at the Web Professionals

Individuals responding to our survey held decision-making roles, either as a solo entrepreneur or with a business or nonprofit.

Nearly 34% of respondents indicated they owned or held a partnership in a small business.

More than 38% said they developed websites for clients, either as a freelancer or the owner of an agency.

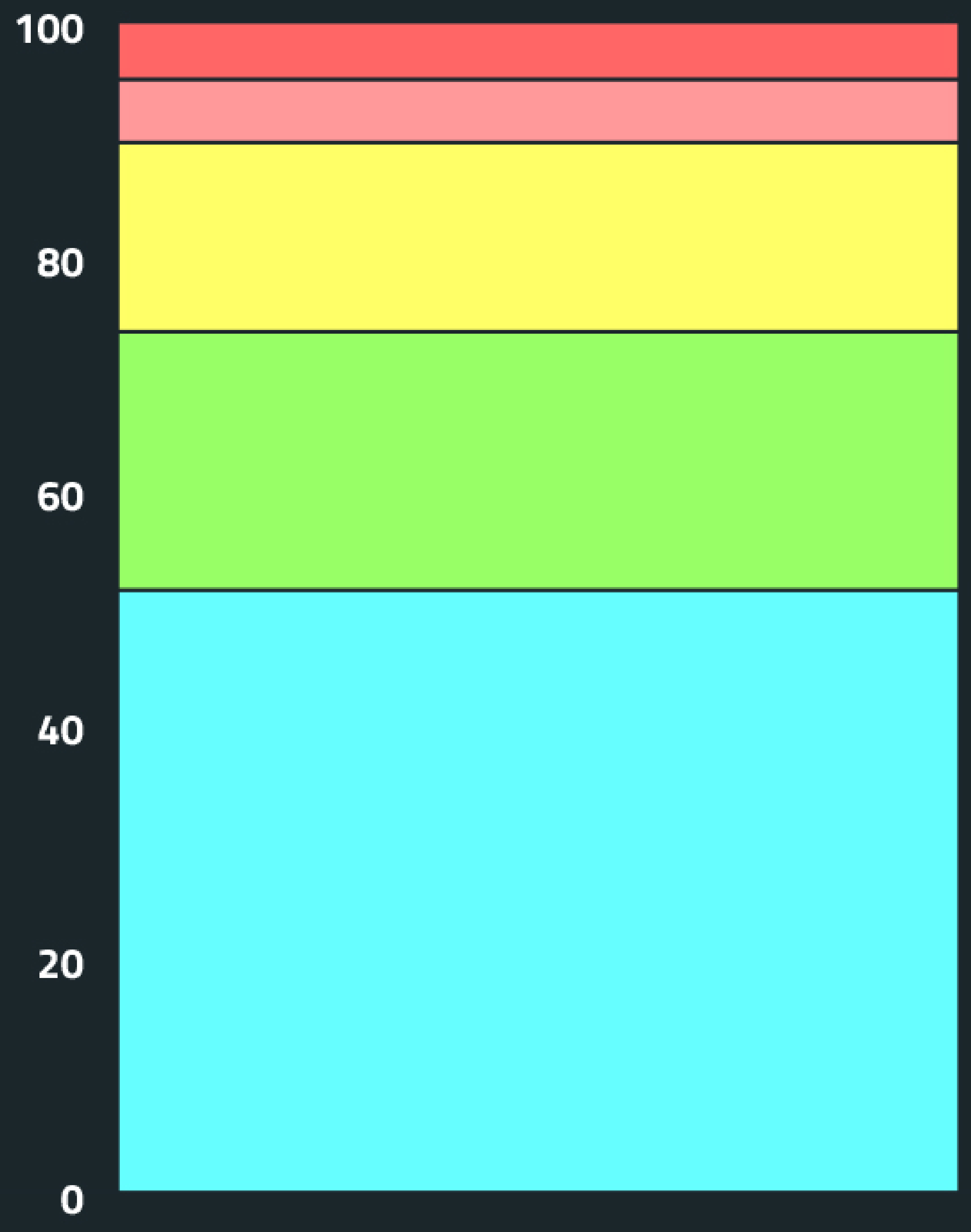
Which of the following best describes you?



Individuals responding to the survey held decision-making roles in their work.

33.66%	I am a small business owner or partner
22.77%	I am a professional website developer or designer either full-time or part-time and get paid by clients for developing websites
15.84%	I work/own an agency that builds and maintains websites for clients.
7.43%	I'm employed by a large/medium enterprise as an inhouse website designer / developer or within the IT department, but this company is NOT an agency
5.94%	I am actively involved in setting up a business or non-profit which I will own and operate
5.45%	Miscellaneous
3.47%	I sell products to my clients such as hosting, domain names, IT products and services but I don't design nor develop websites
2.97%	I am a non-profit founder, director or CEO
2.48%	I often build websites for friends, family or other organizations I am involved with but am not paid for doing so
0.00%	I am a Domain investor – I buy and sell domain names for profit

The scope of their work varied. More than half of our respondents (51.4%) worked on a smaller scale, indicating they handled fewer than eight websites in the past year. About 28% of respondents were midsize operations, with between eight and 50 sites last year. Larger operations, with 51 to 100+ websites, accounted for just over 10% of responses.



More than half of our respondents signaled they were a smaller operation.

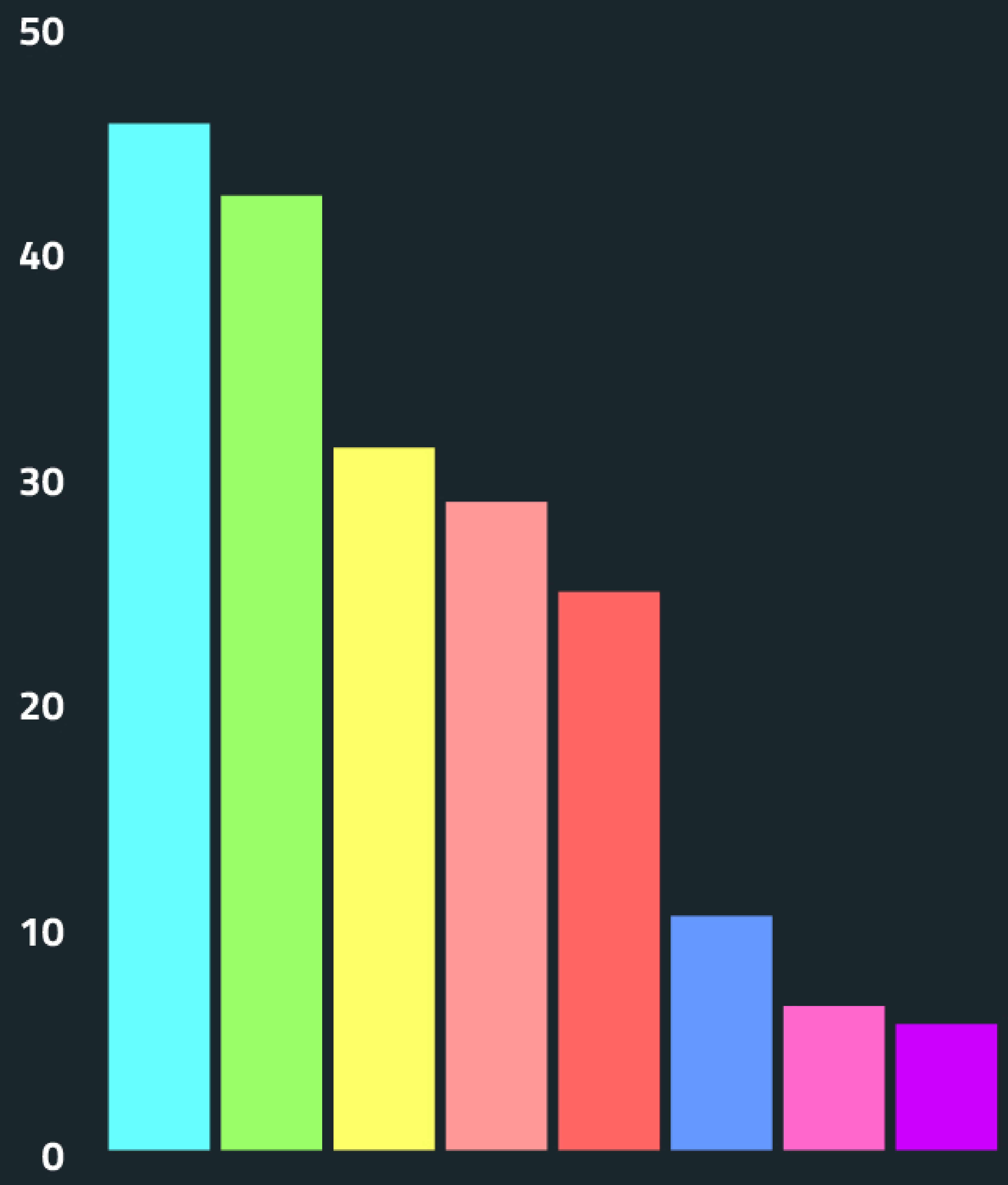
🟥	**4.90%**	100+ websites
🟥	**5.39%**	51-100 websites
🟨	**16.18%**	21-50 websites
🟩	**22.06%**	8-20 websites
🟦	**51.47%**	Fewer than 8 websites

Methods for Securing Websites

Although there remains no fire-and-forget method for securing websites, third-party components like WordPress plugins are becoming more popular for this role. These components often automate routine tasks like scans and backups, reducing the amount of time a person needs to spend on them.

The vast majority of all respondents relied on third-party components or plugins to secure clients' websites, with 46% paying for these components and 42% using free versions. Although larger operations relied on plugins, more than 73% of them indicated they handled some aspects of website security in-house.

How do you currently secure your clients' websites?



■	**5.60%**	I don't have a plan for website security issues
■	**6.40%**	I recommend my clients to use free plugins
■	**10.40%**	I use other methods
■	**24.80%**	I refer my clients to a professional security provider
■	**28.80%**	I handle security issues in-house
■	**31.20%**	I pay professional security provider to cover multiple clients' sites
■	**42.40%**	I use free security plugins
■	**45.60%**	I pay for premium security plugins

Third-party components like WordPress plugins are popular for automating routine tasks.

Methods for Securing Websites (cont’d)

This data aligns with the amount of money that respondents said they were willing to spend each year on website security. More than 79% of all our web professionals said they were unwilling to spend more than $500 — a figure which seemed to remain a benchmark regardless of the size of their operation.

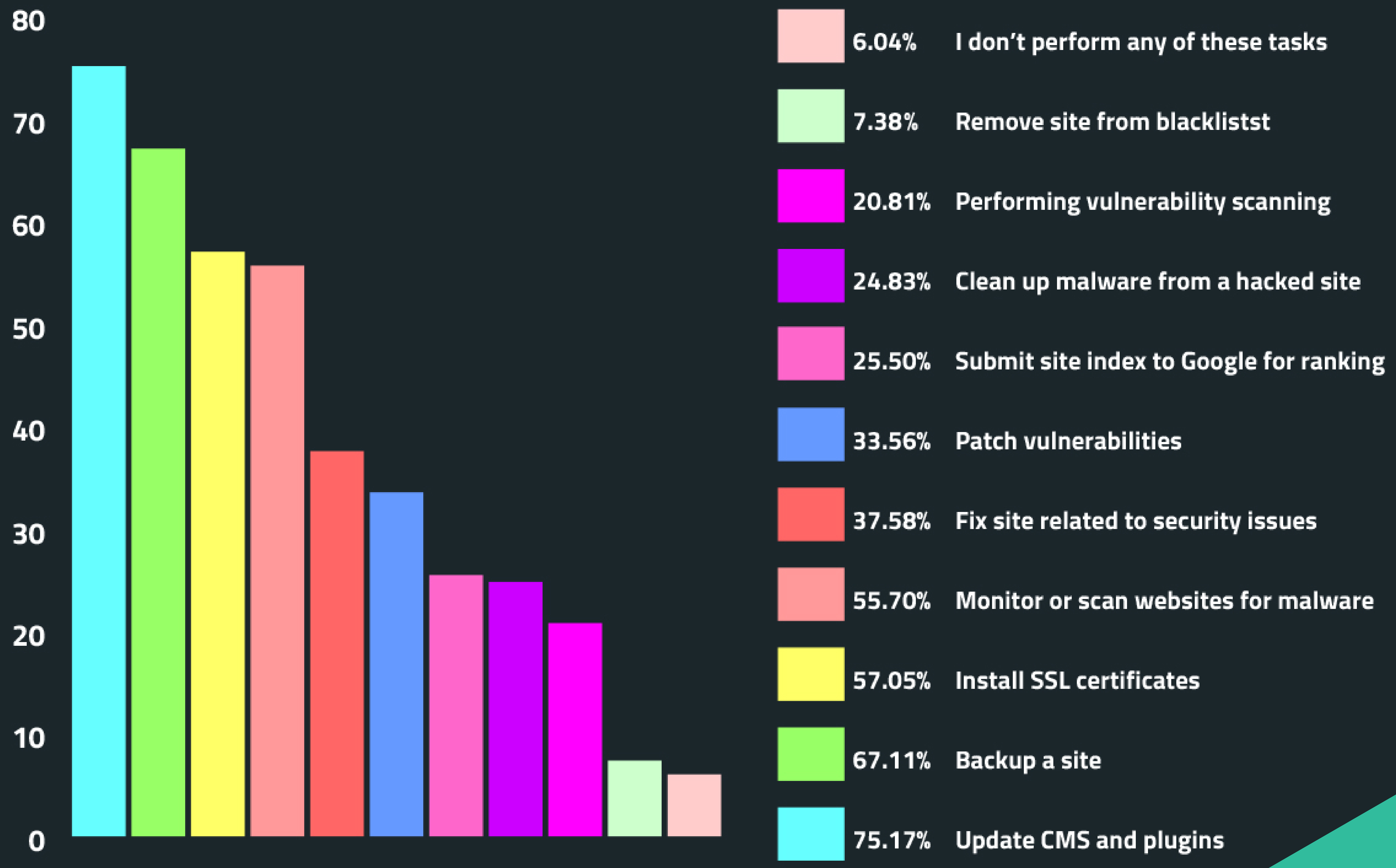
Hands-on Website Security Tasks

For tasks that required some degree of manual interaction, the vast majority of respondents (75%) indicated they handled updates to the CMS and other components. More than 67% also indicated they backed up clients’ websites, while 57% installed SSL certificates and 56% handled scanning and monitoring.

Overall, only a quarter of all respondents indicated they would handle malware cleanup. However, that figure jumped to nearly 59% among larger operations, compared with less than 11% among smaller operations.

What are the top security tasks you perform?

Simpler tasks like updates were more common than complex work like malware cleanup.



Technology recommendations & implementation

Only 2% of respondents indicated they didn't recommend or set up any kind of security products for clients. The majority of our web professionals recommended or set up products including:

- **SSL certificates**
- **Malware removal tools**
- **Firewall for websites**
- **Malware scanners**
- **Backup and restore tools**
- **Password managers**
- **Two-factor authentication**
- **Email anti-spam and anti-phishing**

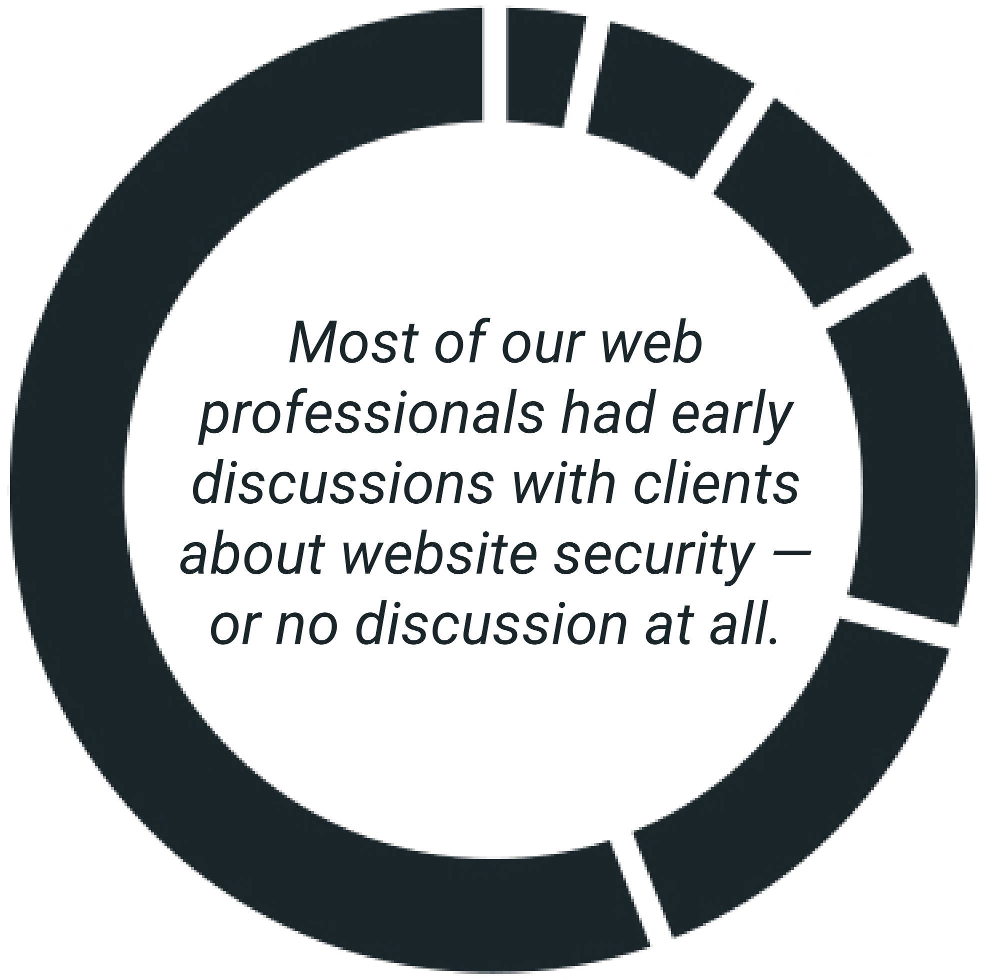
This awareness of website security was echoed in reponses about installing security patches — one of (if not the most) popular attack vectors for bad actors. More than 63% of respondents said they enable automatic updates or install them as soon as possible.

However, these figures shifted among smaller operations, as they mainly relied on automatic updates — or checked weekly (14.8%) if automated updates were unavailable.

Discussing Website Security

A significant majority (66.4%) of all our web professionals indicated they did not need help discussing website security with clients, and nearly 56% indicated having the discussion early, when clients first signed up. However, nearly 15% said they don't talk about website security at all with clients.

When do you bring up the need to add website security with your clients?



Most of our web professionals had early discussions with clients about website security — or no discussion at all.

55.70%	When I first sign up a client
14.77%	We don't talk about website security with my clients
12.75%	When I begin building the client's site
7.38%	When the client site experience a security incident
6.04%	When the client site is published
3.36%	When the client asks me about website security

Discussing Website Security (cont’d)

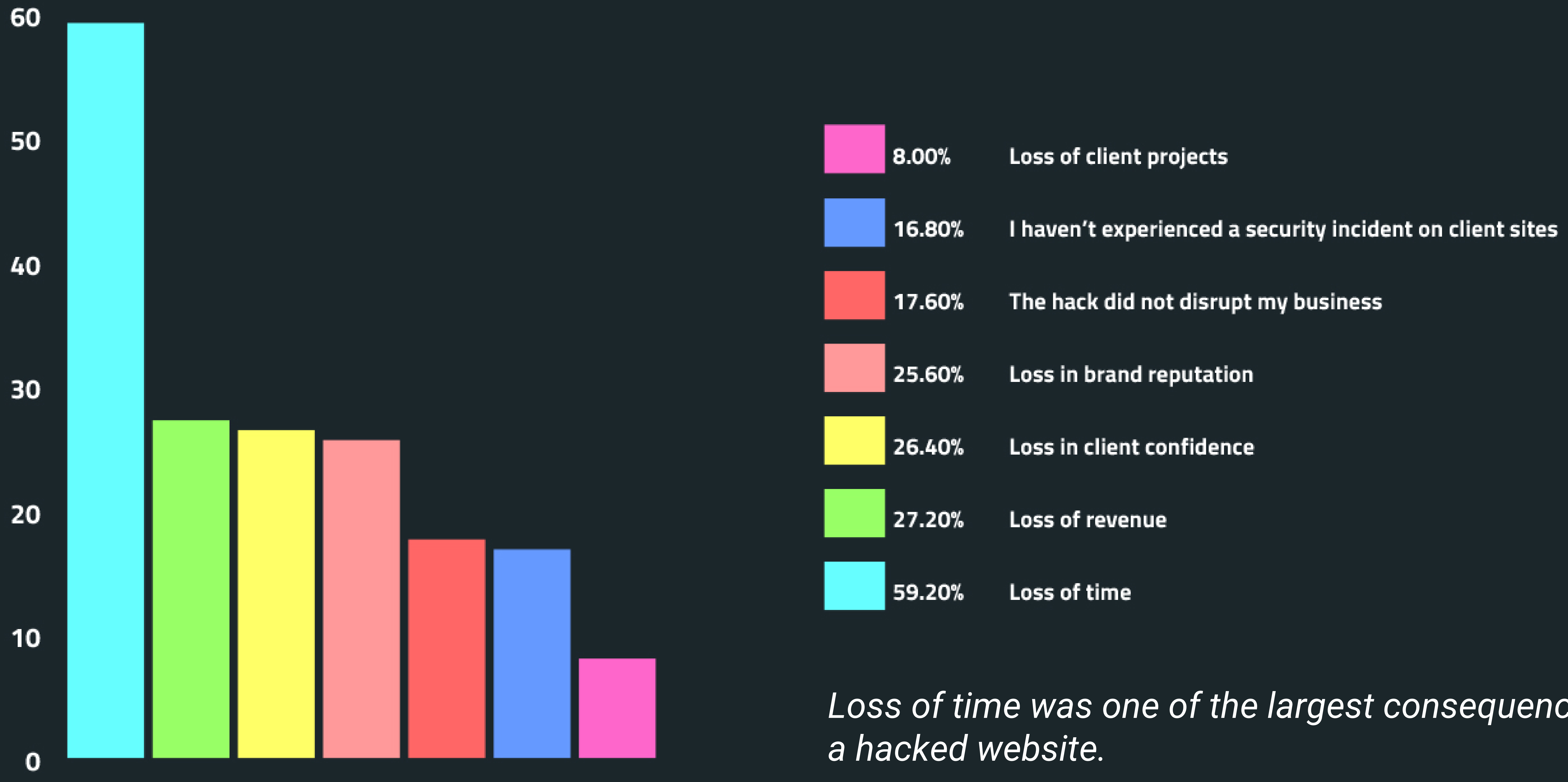
Interestingly, respondents who didn’t discuss website security said that more than 77% of their clients were concerned or extremely concerned about website security — with a third of these clients having experienced a malware infection.

Perhaps unsurprisingly, among respondents who said their clients were unconcerned or extremely unconcerned about website security, nearly 78% had experienced a hack. Hacks took a variety of forms:

- **Search Engine Optimization (SEO) spam**
- **Malware infection**
- **Malicious redirects**
- **Phishing**
- **Comment spam**
- **Blacklisting**
- **Ransomware**
- **DDoS attack**
- **Defacements**

The Impacts of a Hacked Website

Among all of our web professionals, more than 59% said the greatest impact of a hack on their clients was lost time. More than 27% reported a loss in revenue, while damage to their clients’ brands was also an issue — with 26.4% reporting a loss in confidence and 25.6% noting a damaged reputation.



Loss of time was one of the largest consequences of a hacked website.

Conclusion

When it comes to web professionals and website security, there are limitless one-off scenarios and related discussions. This year's Web Professional Security Survey seeks only to expose the tip of the iceberg and, hopefully, spark discussions that ultimately support a safer internet for everyone.

Key takeaways from this report include:

- **We polled decision-makers** — Nearly 34% of respondents indicated they owned or held a partnership in a small business. More than 38% said they developed websites for clients, either as a freelancer or the owner of an agency.
- **Website security remains a low cost priority** — More than 79% of all our web professionals said they were unwilling to spend more than $500 on website security, a figure which seemed to remain a benchmark regardless of the size of their operation.
- **All-in-one solutions are appealing** — The vast majority of all respondents relied on third-party components / plugins to secure clients websites, with 46% paying for these components and 42% using free versions.
- **Security patches are a high priority** — More than 63% of respondents said they enable automatic updates or install them as soon as possible.
- **Hacked websites mean lost time and money** — More than 59% of respondents said the greatest impact of a hack on their clients was lost time. More than 27% reported a loss in revenue, while damage to their clients' brands was also an issue.

sucuri.net

@SucuriSecurity