storyblok

The State of
CMS Security 2022

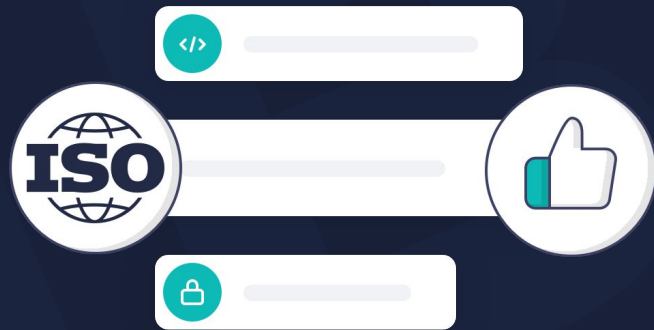**storyblok**

Introduction

💡 As technology evolves, so do the security risks to those who use it

🔓 Storyblok set out to study how enterprise CMS users view and manage these threats

📣 **Main objectives**

- Determine impact of previous threats

- Understand how users prioritize digital safety

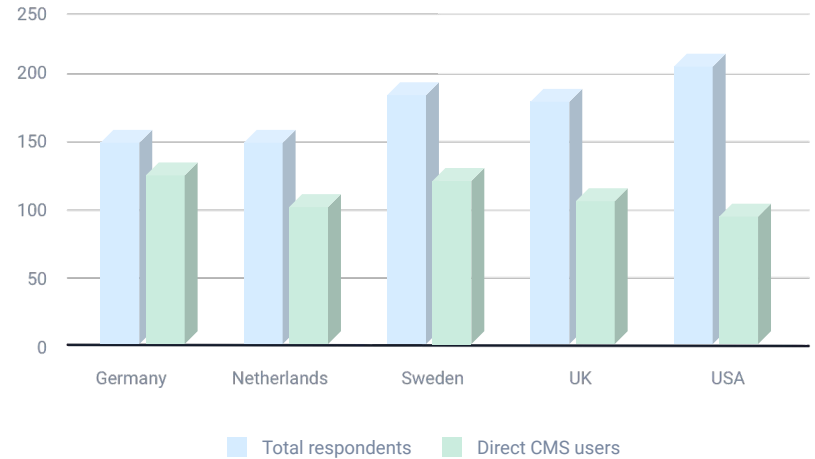- Figure out steps that users take to keep their CMS content secure

storyblok

Demographics

👥 We polled **870** respondents from 5 countries across several industries

💻 **62.9%** personally use a CMS in their organization

Do you personally use a CMS at your organization?

Legend: Total respondents | Direct CMS users

Countries: Germany, Netherlands, Sweden, UK, USA

storyblok

# 64.3% worry about the security of their CMS

- Some common security threats include computer viruses, trojan horses, spyware, and SQL injection attacks

- Security compromises can be costly. Data breaches in the US alone cost $4.24 million in 2021

- Other consequences include compromised content and customers losing trust in the brand

- Most respondents are conscious of how these threats can affect their organization

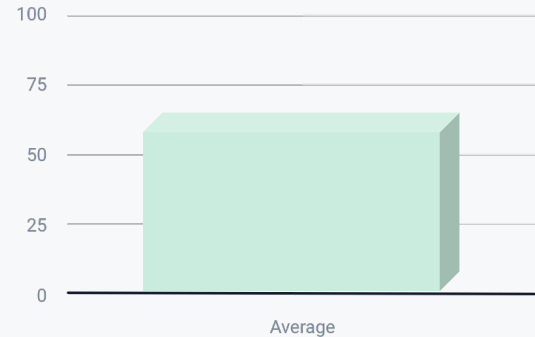### Do you worry about the security of your CMS?

No
35.7%

Yes
64.3%
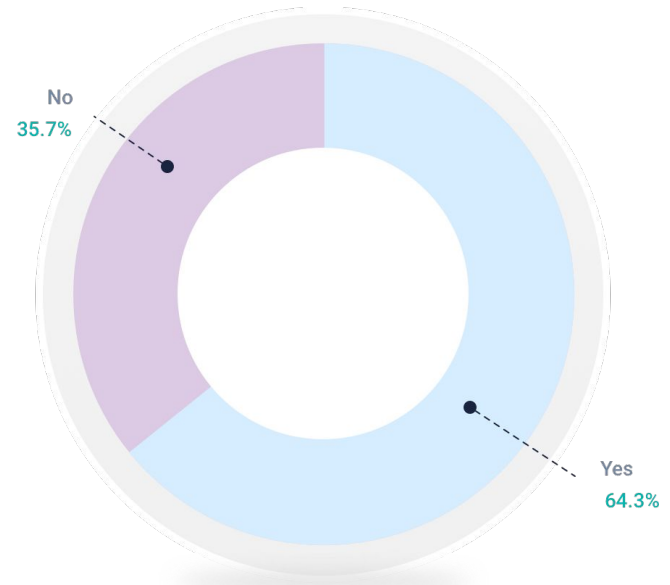
Security threats are a top priority

When choosing a CMS, how important is security to you?

Not so important 2.6%

Not at all successful 1.2%

Somewhat important 16.2%

Extremely important 33.2%
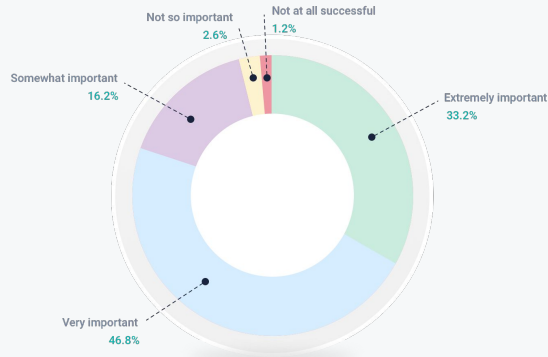
Very important 46.8%

On a scale of 1 to 100, what would be the impact of a security breach / severe security issue for your business?
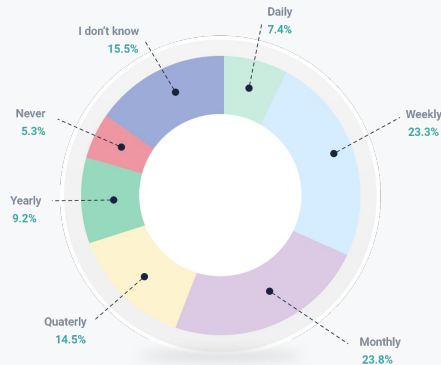

Average

- 80% said security was very or extremely important
  - UK respondents valued it the most with **50.49%** stating it was extremely important
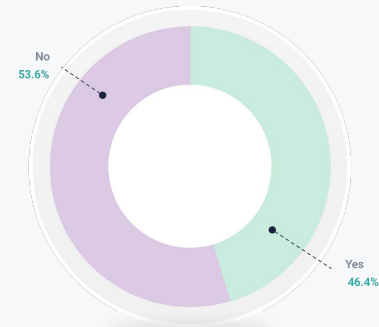- Only **3.7%** of global respondents said it was not so important or not at all important

- On a scale of 1 to 100, the average impact of a security breach / severe security issue was **63.6**
- There was little variation between individual country's answers
  - Germany had the lowest average at **59**, while the UK had the highest at **70**

Security issues and their impact

How often do you conduct security updates per month?

Daily
7.4%

I don't know
15.5%

Weekly
23.3%

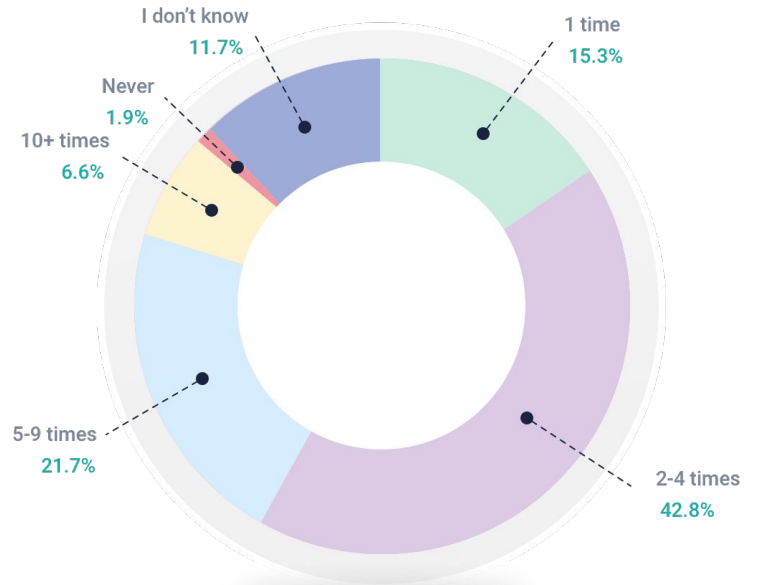Never
5.3%

Yearly
9.2%

Quaterly
14.5%

Monthly
23.8%

- **55.5%** experience new security issues at least monthly
- *That means there's a regular risk for a 63.6/100 degree of severity event to happen to a CMS*
- **20.8%** of respondents either thought they never experience new security threats or did not know the frequency
  - This may suggest that they also do not take the right precautions to prevent them

Has a CMS security issue ever affected your content?

No
53.6%

Yes
46.4%

- Almost half have had security issues affect their content
- Germany had the highest content occurrences at **59.48%**
- **37.89%** of American respondents state that this has happened to their CMS
  - Despite this fact, **9.47%** of them also stated that they never experience new security issues

storyblok

42.8% conduct security updates 2–4 times per month

- Updating a CMS is one of the most important steps in safeguarding it from threats
  - As malicious attacks evolve, CMSs must also evolve to prevent them
- The second most common frequency for updates was 5–9 times per month at **21.7%**

How often do you conduct security updates per month?

I don't know
11.7%

1 time
15.3%

Never
1.9%

10+ times
6.6%

2-4 times
42.8%

5-9 times
21.7%

storyblok

78.1% of respondents think that CMSs take security seriously enough

- Despite this, **64.3% still worry about their CMS security**

  - Sweden had the largest overlap, with **79.31%** having confidence in CMSs yet **70.69%** worrying about security

- This may suggest that CMSs are not always clear about how they plan to protect their users

Do you think CMS providers take security seriously enough?

No
21.9%

Yes
78.1%

storyblok
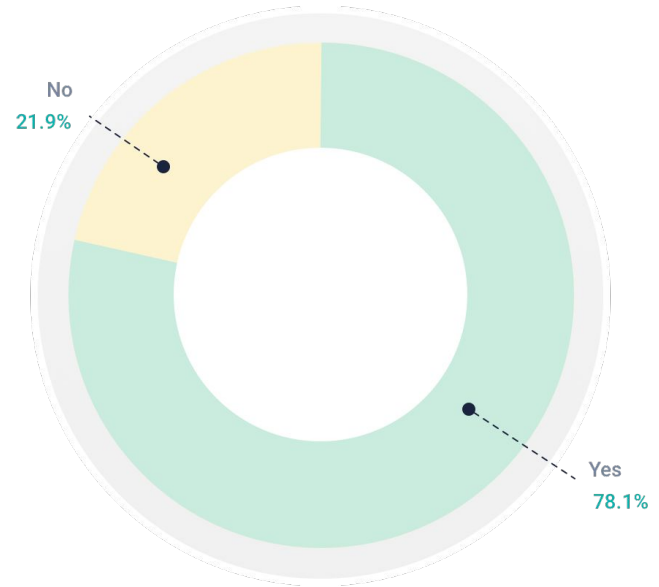
Conclusion

👉 Security is a priority for respondents who cite the consequences and frequency of threats as **relatively severe**

- Most believe CMSs take these issues seriously enough, yet **an overwhelming majority worry about it** nonetheless

👉 **ISO 27001 certification** is an internationally recognized way to confirm that a CMS is ensuring your content's safety to the highest standards

👉 To earn ISO 27001 certification, a CMS must continuously show internationally recognized adherence to safety principles including:

- Encrypted data management
- Risk modeling for potential threats
- A secure software development process per the OWASP code review guide

👉 Certification can help users rest assured that a CMS is taking every possible step to protect their content

storyblok

Your Headless CMS

www.storyblok.com

Storyblok GmbH

Tabakfabrik
Peter-Behrens-Platz 2
Linz 4020
Austria

Northcliffe House
Young Street
London W8 5tt
United Kingdom

Av. Embaixador
Abelardo Bueno 600 - Barra da Tijuca
Rio de Janeiro, RJ, 22775-040
Brazil

Regus Millerntorplatz 1
Aufzug A., 6. Stock
Hamburg 20359
Germany