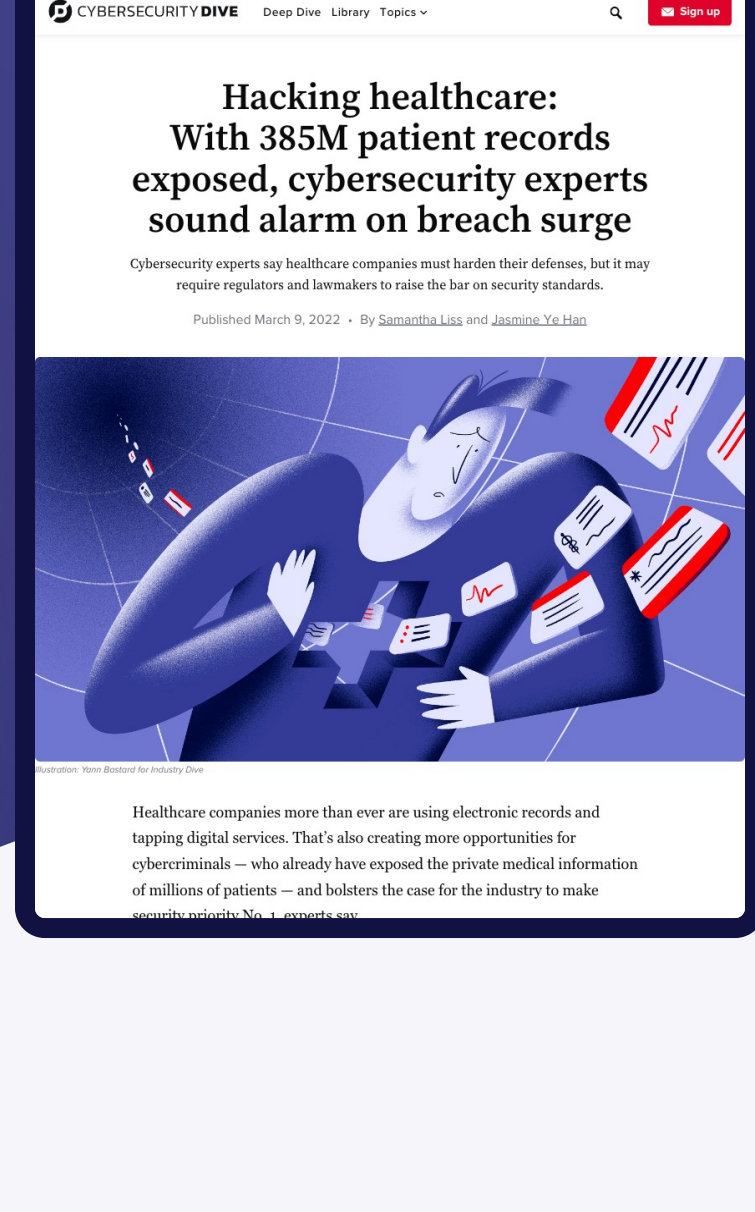


Snapshot

AUDIENCE INSIGHTS FOR 2023



CONTENTS

- 01
AUDIENCE
See who's reading Cybersecurity Dive
- 02
TOP-PERFORMING CONTENT
Uncover top stories, topics, and keywords
- 03
TRENDS
Explore prevailing issues and industry evolutions
- 04
MARKETING INSIGHTS
Lean into the approaches and formats this audience prefers

01 AUDIENCE

34K

unique monthly visitors

69%

of subscribers are manager-level or above

97%

of Fortune 100 companies read Cybersecurity Dive

CYBERSECURITY DIVE

36,300

SUBSCRIBERS

You'll find Cybersecurity Dive's news and insights in the inbox of notable subscribers, like:

- VP & CISO - Quest Diagnostics
- CISO - First Citizens Bank
- VP & CISO - Biogen
- Director of IT Security - Build-A-Bear Workshops
- VP, Information Technology Security Delivery & Operations - Marriott International
- Senior Director of Security Engineering - PepsiCo
- Executive Director of Cybersecurity Engineering - Merck
- VP of Cybersecurity - Target
- Deputy Chief, Enterprise Cyber Defense - DoD
- CISO - The State of Maine

02 TOP-PERFORMING CONTENT

As the world's dependence on technology and automation grows, the strain on the cybersecurity industry rises in tandem. Data breaches and ransomware attacks are becoming the norm and the emphasis on security is more prominent than ever. Cybersecurity leaders are working to keep pace with the rapidly evolving threat landscape by innovating new technologies and security solutions. With new challenges arising daily, let's take a look at what our readers have been focused on most.

Top 5 topics

1. Data breaches
2. Strategy
3. Policy & regulation
4. Vulnerability
5. Identity & access management

Top 10 Cybersecurity Dive stories

What we know about the LastPass breach (so far)

The cybersecurity talent shortage: The outlook for 2023

Cybersecurity trends in 2023 that will directly impact everyday life

Threat intelligence isn't for everyone, Google says

World Economic Forum officials warn global instability could lead to catastrophic cyber event

A first-hand look inside Walmart's robust security operations

What's at stake for 33M compromised LastPass users?

T-Mobile breached again, 37M customer accounts exposed

White House releases national cyber strategy, shifting security burden

Layoffs come for cybersecurity, too

Keywords resonating right now

- generative AI data privacy
- ransomware
- cyber attacks
- data breaches
- artificial intelligence
- vulnerabilities
- LastPass hack
- SBOM executive order
- talent shortage
- layoffs
- cybersecurity trends

03 TRENDS

Industry outlook

- Increased investment in cybersecurity
- Shift to interconnected operations
- Rise in consumer concerns about data privacy

International threats

- Underprepared and underfunded global corporations
- Potential for global instability due to cyber threats
- Push for international cooperation against common threats

Vulnerabilities

- Increased dependence on technology
- Ransomware
- Data breaches

Workforce struggles

- High demand for cybersecurity professionals
- Talent shortage
- Shortage of cybersecurity university professors

Our readers spent nearly 2x as long on these stories than the average story:

- [Google Cloud joins FS-ISAC's critical providers program to share threat intel](#)
- [Box CEO on the 'perfect storm' of challenges in cybersecurity](#)

The new normal: data breaches

Following the pandemic, supply chain dependence on automation grew, increasing corporations' risk of potential ransomware attacks and data breaches. In recent years, several prominent companies have been under attack, leaving no one safe from actors.

Cybersecurity costs are expected to grow to a record high in 2023 with a surge of cyber attacks. Although most cybersecurity executives expect their budget to grow in the coming years, underinvestment has been a factor plaguing the industry for years and could continue to as the market navigates economic uncertainty.

Cybersecurity as a global issue

A major concern in cybersecurity is the vulnerability of global corporations in the event of a wide scale cyber attack. In the next few years, industry sources see potential for major global instability in the event of a catastrophic cyber attack.

Global corporations' dependence on technology and the increasing complexity of the cyber environment leaves them vulnerable and unprepared in the event of an attack. Cybersecurity leaders are realizing that cybersecurity is a global problem that should be tackled with collaboration and coordination across global entities.

A wavering workforce

The waves are higher in cybersecurity as threats and the demand for cybersecurity professionals are changing than ever before. However, with fewer young professionals entering cybersecurity than needed, the industry is facing a shortage of essential employees to keep corporations secure.

Although the cybersecurity workforce was at its peak in 2022, a lack of interest in the cybersecurity field and a shortage of university cybersecurity professors both contribute to the current shortage. However, this hasn't stopped some prominent corporations from laying off percentages of their workforce to tighten spending.

04 MARKETING INSIGHTS

Authenticate your audience strategy by reflecting the content preferences of over 36,300 Cybersecurity Dive subscribers in your strategy:

Content Characteristics

- Concise
- Poignant
- Tactical
- Solutions-oriented
- Global

Content Types

- Insights on overarching trends via trendlines
- All-encompassing and on-demand resources like playbooks
- Interactive content like webinars

Spotlight top talent

Cybersecurity leaders are on the lookout for innovative ways to improve their operations and enhance their security. From forensics labs to information security departments to retention and talent strategy, executives want to mirror the best of the best. Use top brand names in case studies and headlines to drive engagement.

Don't overlook the day-to-day threats

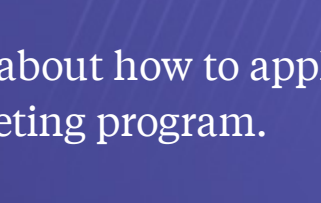
While advanced cybersecurity threats are a global issue, the majority of companies are facing email compromise, phishing, and zero-day vulnerabilities. Create content geared toward their interests and concerns that are just as tactical and comprehensive as the big players.

Aid leaders in quick decision-making

These leaders don't have time to spare, especially in the event of an emergency. Help them overcome the obstacles they face daily by providing them with information on comprehensive, actionable solutions. Be sure to always use and cite authoritative sources to earn this audience's trust.



studio / ID



How are you resonating with this audience?

Contact us for more details about how to apply these insights to your marketing program.

Contact us