CYBERSECURITY DIVE

Snapshot 2024

AUDIENCE INSIGHTS

Cybersecurity Dive is a news publication designed specifically for cybersecurity leaders overseeing information and network security for their company. Across ransomware attacks, security breaches, IT resources, and remote network safety, our journalists cover the issues that impact cybersecurity.

01 Audience

70K
unique monthly visitors

70%
of subscribers are *manager-level or above*

97%
of Fortune 100 companies read Cybersecurity Dive

CYBERSECURITY DIVE

48,000

SUBSCRIBERS

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

- CISO, General Motors
- VP & CISO, Quest Diagnostics
- VP of Cybersecurity, Target
- VP & CISO, Biogen
- Sr. Director, Cybersecurity, Hilton Worldwide
- Sr. VP of Risk Control Data Management, Bank of America
- VP of Information Technology & Security, Starbucks
- CISO, The State of Maine
- VP, IT Security Delivery & Operations, Marriott International
- VP of Global Information Tech & CISO, Medtronic

02 Top-performing content

Between debilitating supply chain attacks, international fallout in war-torn countries, and everyday exploitation, companies are on guard to defend against external cyber threats coming from all sides. Risk mitigation and regulatory compliance have never been more critical enterprise priorities. Let's take a look at what cybersecurity leaders have been focused on most.

Top 5 topics

- Cyberattacks
- Breaches
- Policy & regulation
- Strategy
- Vulnerability

Top 10 Cybersecurity Dive stories

1. First American Financial confirms threat actors stole and encrypted data
2. 5 cybersecurity trends to watch in 2024
3. Microsoft to overhaul internal security practices after Midnight Blizzard attack
4. Progress Software's MOVEit meltdown: uncovering the fallout
5. Okta, with a bruised reputation, rethinks security from the top down
6. CISA, FBI confirm critical infrastructure intrusions by China-linked hackers
7. How to ensure data privacy in a ChatGPT world
8. CISA's 1,200 pre-ransomware alerts saved organizations millions in damages
9. What's ahead for cybersecurity in 2024
10. Mortgage industry attack spree punctures common errors

Keywords resonating right now

- recent ransomware attacks
- cybersecurity incident response and reporting
- US cyberattacks and breaches
- AI cybersecurity risks
- firewall exploits
- critical infrastructure security
- compliance regulations
- third-party vendor targeting

03 Trend analysis

Vulnerability at an all-time high

- Hackers increasingly aim at high-value and high-profile targets that are more likely to pay ransom demands.
- Rise in volume of attacks targeting third-party vendors to amplify ripple effects and disrupt supply chains
- Enhanced exploitation of common entry points (remote desktops, phishing or malware, and software vulnerabilities) and emergent territories (IoT, AI/machine learning, etc.)

More stringent rules & regulations

- Increased regulatory scrutiny and new, more intense requirements to report cybersecurity threats in an effort to share more intel and prevent internal and external spread
- State and Fed putting pressure on companies to tighten technical expertise, increase incident reporting, and quicken response time to malicious activity
- Regulators crack down on protections for sensitive consumer data, particularly for entities like insurance companies and banks

All-in on proactivity & prevention

- Increased emphasis on applying preventative measures in the early design/development stage (memory-safe languages, AI-based code auto-fix feature, etc.)
- Heightened security for mobile devices (move away from authentication via SMS + phone call; move into app-based multi-factor authentication and security keys)
- Push for guidance and policies surrounding employee use of generative AI tools to decrease risk of internal data breaches; focus on thwarting AI-driven external attacks

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

- Change Healthcare cyberattack having 'far-reaching' effects on providers
- At, fake CFOs drive soaring corporate payment-fraud attacks

Supplementing with AI

Some developers lean on AI for code generation, while security is wary of vulnerability-riddled code — leaving reservations across IT domains.

studioID tip

Showcase AI as an "ingredient" in the larger "recipe" of how developers leverage GenAI-generated code. Follow the same idea — what small piece does AI play in larger IT and cybersecurity contexts? Acknowledging the benefits while weighing the risks will help ease the burden of GenAI adoption and integration.

Cybersecurity's presence in the boardroom

No longer siloed within just IT, cybersecurity is now a top-level, strategic priority. Board members want to see how their cybersecurity investments are delivering.

studioID tip

Cybersecurity ROI is historically difficult to measure. Essentially, a year without an attack or breach is a sign of success — but there's many more performance indicators to convey. Help cybersecurity professionals communicate the connection between stakeholder investments and preparedness in ways that resonate with the boardroom.

Evolving guidance and regulation

As cyberattacks have become more sophisticated over the last decade, the federal government has marketed itself as an ally for recovery.

studioID tip

Federal agencies want the private sector to lean on it for guidance, support, and direction before and after an incident. They are dependent (and desperate) for a private-public sector relationship. Assist cybersecurity leaders in ensuring compliance and effectively engaging with these agencies (including law enforcement like the FBI).

04 Marketing insights

Authenticate your audience strategy by reflecting the content preferences of over 48,000 Cybersecurity Dive subscribers.

Preferred content types

- Webinars/virtual events
- Trendlines
- Playbooks
- Infographics

High-impact approach

Lean on trustworthy SMEs

In the complex world of cybersecurity, professionals want to hear from credible sources — think boots-on-the-ground experts.

studioID tip

Cybersecurity leaders are often swept up in the bigger picture strategy, not day-to-day operations. Earn their trust and help them keep pace with best practices by delivering small straight from experts within the field. While industry vets are always highly regarded, don't forget about all of the value the tech-wiz newcomers have to offer as well.

High-impact approach

Deliver clear-cut guides

CIO and CISO roles have recently shifted to a business-savvy, strategic role. Make their lives easier with play-by-play guides.

studioID tip

Guides and playbooks are popular with cybersecurity leaders who want to know evidence-based, stepwise instruction. Lay out the stages of a process and use mini case studies or use cases to support your points. Give insight into how a CIO/CSO can resonate with their non-technical C-suite counterparts.

High-impact approach

Revolve around regulatory changes

In the last four years alone, different industries have been instructed to adopt regulations (think TSA's guidelines following the Colonial Pipeline hack). How has progress been?

studioID tip

Explicit cybersecurity regulations are now the norm as regulatory agencies, and even the White House, are calling for stricter policies. Address how companies are measuring up, how specific industries are implementing changes, and examples of how industries are modernizing their tech stack. Go a step further and speak about those challenges and how to overcome them.

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