origin
communications

The Changing Face of Information Security Media Consumption in 2024

February 2025

Narrative Report

Methodology

The research was conducted by Censuswide, among a sample of 251 C-Level Professionals with responsibility for information security (25+). The data was collected between 29.11.2024 - 03.12.2024. Censuswide abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Censuswide is also a member of the British Polling Council.

IT/technology websites are read and used most frequently by infosecurity C-Suite (59%) compared to other sources

When it comes to IT security, infosec C-Suite read or use the below most frequently:

IT/technology websites (59%)

IT security specific websites (55%)

IT security specific magazines (physical and online) (43%)

A notable proportion of respondents also read and use the following, so prove to be valuable sources of information:

- Vendor websites (19%)
- Video websites (17%)
- Podcasts (16%)
- IoT devices (16%)
- General news websites (12%)

Less commonly, infosecurity professionals said that they read/use the opinions of:

1. Peers (9%)
2. Newspapers (website) (8%)
3. TV news channels (7%)
4. Newspapers (print) (6%),
5. TV documentaries (6%),
6. Blogs (5%)
7. General magazines (physical and online) (4%)

These lower percentages do not mean these types of media need to be dismissed entirely, as the survey asked the sources used most frequently, but are perhaps less of a priority.

Newspapers (print) (6%),

TV news channels (7%)

Looking specifically at websites, the **10 most common read/used for IT security by respondents are**:

1. ITPro. (32%)
2. CYBER SECURITY INTELLIGENCE (32%)
3. ITSECURITY WIRE (28%)
4. TechCrunch (24%)
5. BBC NEWS (24%)
6. Bloomberg (24%)
7. CYBER DEFENSE MAGAZINE (24%)
8. FINANCIAL TIMES (24%)
9. intelligent CISO — security intelligence that transcends borders (23%)
10. The Economist (23%)

For full list, please visit and download the report, available on the website: www.origincomms.com

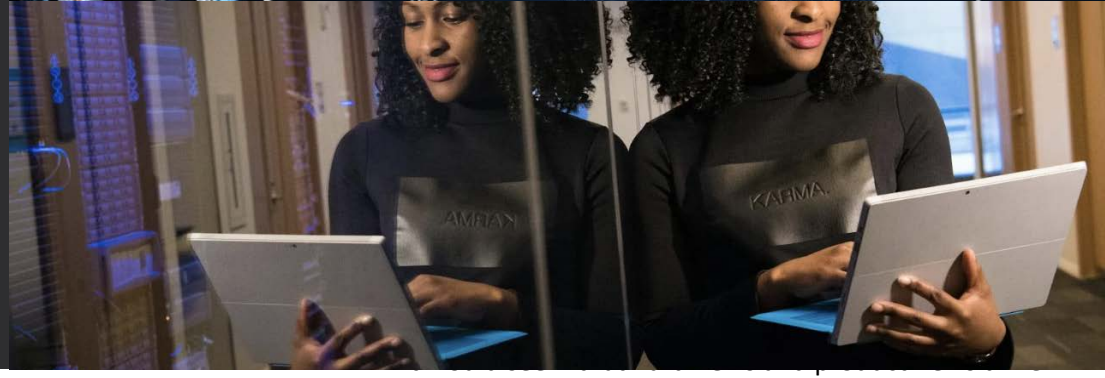
Now looking at newspapers/magazines/supplements read/used for IT security, the top five are:

1	2	3	4	5
Cyber.	Computing Security	FINANCIAL TIMES	The Guardian	The Economist
(42%)	(41%)	(35%)	(33%)	(31%)

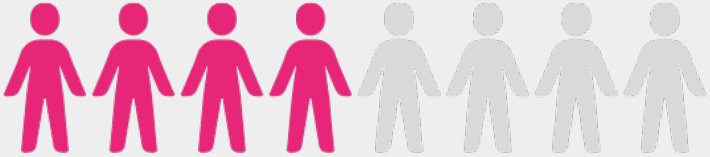
These were closely followed by:

- The Telegraph (31%)
- The Times (29%)
- The Daily Mail (24%)
- The Sun (23%)
- The Independent (22%)
- Daily Express (21%)
- The Metro (20%)
- The iNews (19%)
- The Standard (19%).
- The Mirror (16%)
- City A.M (14%)
- Raconteur (14%)

The top 3 drivers for infosecurity C-Suite to view IT security content:



respondents to engage with content but also a need from a job role perspective, which suggests that content is a key part of decision making when it comes to seeking new vendors or suppliers.



Half (50%) of respondents say legislation change (e.g. GDPR) is what drives them to view/access IT security content.

Followed by

- Industry change (47%)
- Personal interest (46%)

Less likely drivers are:

- Competitor announcements (36%)
- Recommendations from peers (35%)

Trust and distrust in platforms

The five sources/platforms' respondents feel are the most trustworthy for sourcing IT security content are:

- IT security specific websites (48%)
- IT/technology websites (48%)
- IT security specific magazines (physical and online) (44%)
- Advisory boards (e.g. ISACA, NCSC, NCAB, IAAC) (30%)
- LinkedIn (19%)

The five sources/platforms' respondents feel are most likely to spread misinformation or manipulated content are:

- TikTok (36%)
- Facebook (35%)
- Twitter (27%)
- Instagram (24%)
- Blogs (17%)

Vendor Selection
Influences

Respondents are slightly more likely to be influenced by articles written about the brand or product at the stage where they are choosing to buy (34%) than the stage where they are engaging (31%), which highlights the importance of PR at the critical stage of purchase decision making.

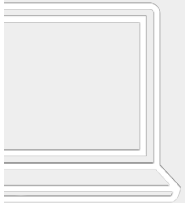
Exploring how respondents are influenced at two key stages of the marketing funnel, it's notable that past experience with a brand is the top influence both for engaging with a vendor (51%) and choosing which product/brand to buy for their organisation (59%).

Reviews written by users is the second most impactful influence for both engaging with a vendor (48%) and choosing which product/brand to buy for their organisation (48%), whilst reviews written by a third party is the third most impactful for both engaging and choosing (both 39%).

The sources that are most likely to influence respondents' organisations in changing vendor/suppliers are:

IT security specific websites (48%)

IT/technology websites (42%)



IT security specific magazines (35%)

These types of sources often coming up in the most selected in a variety of questions demonstrates their influence

We've seen the power that content can have in influencing decisions, so it's important to explore what it is that respondents want from this content

Infosecurity C-Suite consider **expert voices** most important (16%)

When evaluating the reliability of content, infoSecurity C-Suite consider these to be the most important:

Expert voices - hearing directly from CISOs, CSOs, and other security leaders (16%)

Source credibility (15%)

Fact-checking and references (12%)

When deciding whether to trust and engage with content, these top three remain the same:

15% Expert voices; 14% Fact- checking and references; 10% Source credibility

Negative Influences

As well as positive influences, it's important to explore what can negatively impact purchasing decisions.

Poor information on the website (52%) is the top factor that would put respondents' organisations off buying a product

Other negative influences include:

A lack of customer support (47%)

High pricing (43%)

News of a breach (41%)

Low online presence (31%)

For full list, please visit and download the report available on the website: www.origincomms.com

Event Influences

Networking receptions or social gatherings (75%) and executive summits or C-level forums (75%) are the most popular types of events for cybersecurity goals

Events are another **key way to engage with target audiences**

The top 6 factors respondents deem important* when deciding to attend, host, or exhibit at cybersecurity events are:

Ability to **research industry trends and competitors** (89%)

Overall **reputation of the event** (88%)

Brand visibility and exposure (88%)

Followed by:

- Showcase of new products or services (86%)
- Relationship-building opportunities (86%)
- Potential to attract new customers (86%)

*** Extremely important and very important responses combined. For full list, please visit and download the report available on the website: www.origincomms.com**

Looking at this by '**extremely important**' alone, respondents place the highest importance on overall reputation of the event (56%) and the least importance on flexibility with time and attendance (for virtual events) (35%) or expected number of attendees (35%).

Respondents place the highest value on overall **reputation of the event**

The below outlines the **types of events** respondents find most beneficial for achieving various cybersecurity goals

GOAL: Building Strategic Partnerships and Relationships

- Executive summits or C-level forums (29%)
- Networking receptions or social gatherings (24%)
- Security conferences (23%)

GOAL: Enhancing Brand Visibility

- Industry trade shows (26%)
- Networking receptions or social gatherings (25%)
- Educational workshops or training sessions (22%)

Executive summits & C-level forums ranked best for building strategic partnerships

GOAL: Knowledge-Sharing and Thought Leadership

- Executive summits or C-level forums (22%)
- Security conferences (22%)
- Webinars and online panel discussions (21%)

GOAL: Driving Customer Engagement

- Virtual meetups or online communities (21%)
- Product launch events or demonstrations (20%)
- Networking receptions or social gatherings (20%)

GOAL: Recruiting Cybersecurity Talent

- Educational workshops or training sessions (22%)
- Security conferences (21%)
- Webinars and online panel discussions (20%)

Educational workshops or training sessions are most effective for recruiting cybersecurity talent

GOAL: Networking with Regulators and Policy Experts

- Executive summits or C-level forums (27%)
- Roundtable discussions with industry leaders (21%)
- Security conferences (20%)

GOAL: Showcasing Innovative Solutions and Services

- Product launch events or demonstrations (23%)
- Industry trade shows (22%)
- Webinars and online panel discussions (21%)

GOAL: Improving Incident Response and Recovery Strategies

- Security conferences (24%)
- Educational workshops or training sessions (21%)
- Roundtable discussions with industry leaders (18%)
- Virtual meetups or online communities (18%)

Security conferences are most effective for **improving incident response and recovery strategies**

GOAL: Exploring Emerging Technologies

- Industry trade shows (25%)
- Security conferences (20%)
- Executive summits or C-level forums (20%)

GOAL: Securing Funding or Investment Opportunities

- Security conferences (23%)
- Executive summits or C-level forums (22%)
- Industry trade shows (20%)

Security conferences were ranked highest for securing funding or investments

What information do infosecurity C-Suite want in times of crisis?

The specific types of information respondents do, or would find most valuable and actively seek to inform their response in the event of an incident are:

1

Immediate threat details – Nature and origin of the threat, type of attack, and affected systems (26%)

Threat intelligence updates (26%)

2

Affected systems and data – Which systems, data types, or business areas might be compromised (22%)

3

Recovery plans (21%)

Legal and compliance guidance (21%)

Cybersecurity **Content – the impact of AI, top themes and topics now and in 5 years' time**

Respondents are almost 3x more likely to think AI will improve content quality than dilute the quality (49% vs 17%)

Themes, topics and information sourcing

Cybersecurity themes/topics infosecurity C-Suite most want to read about in 2024/25 are:

AI governance and ethics (11%)

AI and machine learning (10%)

Cybersecurity skills gap and workforce development (7%)

Meanwhile, the cybersecurity themes/topics respondents see as most critical within their organisation and tend to seek further information on regularly are:

AI and machine learning (10%)

Cybersecurity skills gap and workforce development (9%)

Cyber resilience incident response planning (6%)

Looking to the future, the cybersecurity themes/topics respondents think will top the agenda in five years' time are:

AI and machine learning (13%)

AI governance and ethics (12%)

Cybersecurity skills gap and workforce development (6%)

What's clear is that **AI is, and will continue to be, a big topic** for the infosecurity C-Suite

AI-generated content

When asked how they think the rise of AI generated content will impact the quality of information available on cybersecurity topics and/or the way the consumer will evaluate this content, almost half (49%) believe AI will improve content quality, which was the top answer.

Respondents were also more likely to think it could enhance personalisation (32%) than say they are concerned about misinformation (27%), be more sceptical about it (19%) or think AI will dilute content quality (17%). So, respondents are almost more likely to think AI will improve content quality than dilute the quality (49% vs 17%).

Infosecurity C-Suite seem to view **AI generated content much more favourably** than unfavourably, almost half (49%) believe AI will improve content quality.

If you would like to discuss any of the findings in this report or how we can support you, please do get in touch:

Origin Comms
Devon House
3 High Street, Thames Ditton
Surrey KT7 0SD
T: 020 3814 2940
E: team@origincomms.com

www.origincomms.com

origin
communications