



wildfire

「Think® Bold」

Think first.

The status quo sucks. Doing what you've always done just isn't going to cut it. But doing something for the sake of doing it, with no foundation in a meaningful strategy, will never deliver the results you want. We believe every campaign needs a brand platform that challenges preconceptions and outsmarts the competition. It's why our team of consultants will always think first, always ask questions, and always...

Be bold.

Being bold isn't about being flashy. It's not about hype. It's about being confident in pushing the boundaries because you've done the hard work. Because when you know what really matters, being bold isn't a risk. It's the only way to truly stand out and deliver the campaigns that will make a real impact on your business.

Who is the CISO?



Getting to know the CISO

Your target audience in numbers

The best campaigns are not designed around your product, they are designed around your target audience. But how much do you really know about the CISO?

Do you understand who they are, what they care about, what drives them, and who influences their decision making?

As part of our Think.Bold process we don't leave these questions to chance – we ask CISOs directly.

This book presents critical insights into the mindset and behaviour of the CISO — drawing on one-to-one interviews, qualitative research, and our own survey of 100 decision makers. Our aim is to help marketers and comms professionals at IT, security, and cybersecurity firms understand one of the most influential decision makers in the security buying journey — the CISO.

35-44

Typical age of a CISO

3

Companies worked for

80%

Are the final purchase decision maker

6

Average years in role

25

Average years working in tech

67%

Have stayed in the same industry

What's the CISO personality?



Understanding the CISO

Focus on the facts

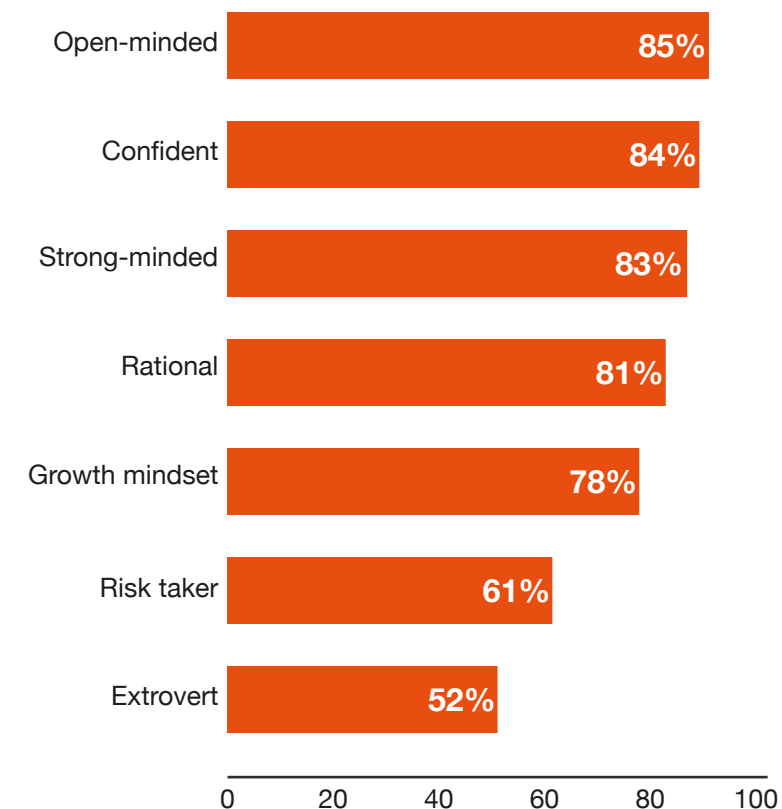
The top career goal for CISOs is to be successful. They want to win, but they don't want to achieve this by taking big risky bets.

CISOs aren't afraid of a challenge (it's a top priority when looking for a new role) and they are open to new ideas. However, they want to make rock solid decisions – especially as over half (51%) of them are the sole decision-maker when it comes to buying in new technology. They want to be right rather than first.

Four out of five CISOs prefer a rational, fact-based approach to decision making. They aren't going to be persuaded by 'fluff'. They want evidence, they want proof, they want to see your credentials.

If you want to make an impact with the CISO, show them how you share this empirical, evidence-based approach.

CISO personality traits



What do CISOs care about?

Priorities and challenges

A complex threat landscape

It's fair to say the CISO has got a lot to worry about: maintaining compliance with increasingly stringent data privacy regulations; fighting off nation state attacks; daily fundamentals like making sure staff are observing cybersecurity best practice when using company systems.

On top of that is the sheer pressure they're under. If something does go wrong, it's not a minor inconvenience. It leads to fines, it affects share prices, it scares customers away.

The role of CISO is a delicate balancing act between internal and external pressures, technological and operational challenges.

So, if you're not here to help then you can probably give up trying to connect with the CISO.

Getting the CISO to buy in is about showing how you solve their biggest challenges. It's not about your spec sheet or your latest software widget. In short – how are you going to make their life easier?

Top challenges for the CISO

- Performance limitations (66%)
- Outdated infrastructure (63%)
- Lack of budget (61%)
- Post-breach brand perceptions (61%)
- Lack of trust in automation (60%)

Who influences the CISO?

Influences and peers

Individual decisions, in a shared process

The majority of CISOs are self-starters. They're not looking for validation from their peers. In fact, feeling appreciated and valued ranks as their lowest priority in carrying out the CISO role.

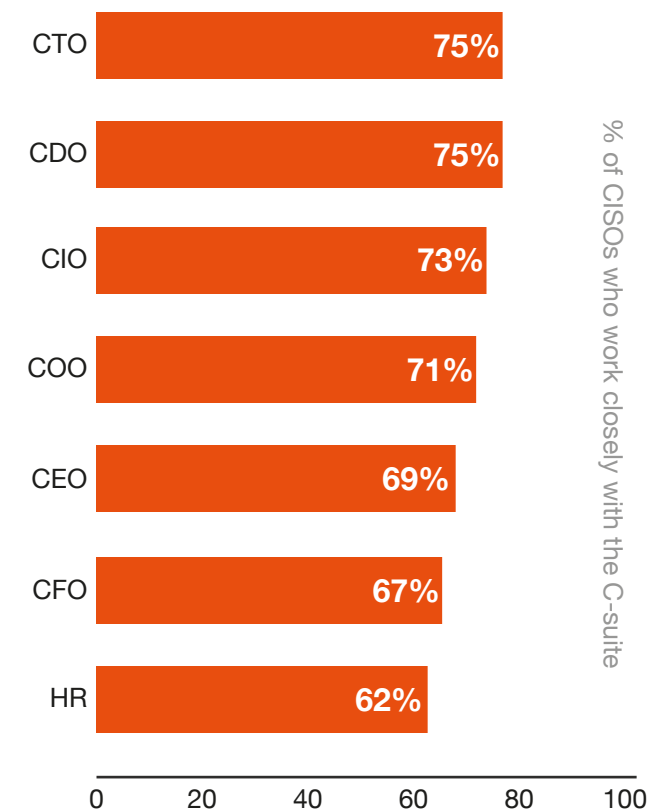
But that doesn't mean they're not working closely with the rest of the business. While the data shows that CISOs are primarily looking for technical collaborators — the CTO, the CDO, the CIO — that doesn't mean they aren't looking for buy-in from other departments.

Indeed, one of the CISO's biggest frustrations is a lack of C-suite buy-in for their plans.

So ignore these peer relationships at your peril. Reaching the CISO doesn't mean focusing solely on them.

If you can broaden understanding of the complex cybersecurity challenges facing the business to other C-level executives, then you can become a crucial ally for the CISO — not just a supplier.

Who works closely with the CISO?



How do CISOs buy tech?



Selecting IT and cybertech

Data, proof, and evidence are king

CISOs don't believe in silver bullets, and they don't believe over-ambitious sales pitches promoting any one technology as the answer to all their prayers.

They are all too aware that any tech they buy will be part of a broader ecosystem or infrastructure. Indeed, 'integration with other technologies' is their most important criteria for selecting cybersecurity technology.

When it comes to choosing a technology partner, CISOs want proof, proof, proof. Have you done this before? Where? How recently? What partners and technologies do you have experience working with?

CISOs also seek out and solicit opinions and recommendations (particularly from analysts).

What's most important when choosing a tech partner?

- Proven capability (89%)
- Cutting-edge technology (89%)
- Analysts' opinions (85%)
- Suppliers that match their ambition (85%)
- Recommendations from CISOs (84%)
- Proven experience with similar businesses (83%)
- What media say about the company (71%)

How do CISOs research?



Finding new tech suppliers

Leaving no stone unturned

At this stage it might be an unsurprising revelation that the CISO takes due diligence of new technologies seriously. They're not going to buy simply because they saw the vendor's CEO quoted in The Times.

CISOs will attend events, delve into multiple analyst reports, ask fellow CISOs for suggestions, and read what the most respected technical journalists say.

Four in five CISOs are going to interrogate your website, so you'd better make damn sure it's easy to find the information they are looking for. Provide proof and data, like product specs and case studies, and make sure it's available across multiple channels.

CISOs will make the effort to get as complete a view as they can of the available technology options — and you need to be where they are.

Where do CISOs go for tech recommendations?

- Online events **(45%)**
- Vendor websites **(42%)**
- Analyst reports **(39%)**
- Search engines **(37%)**
- Personal recommendations **(33%)**
- LinkedIn **(33%)**
- Trade and business media **(29%)**

Are CISOs on social media?

The social CISO

How do CIOs use social media?





Social media isn't just for consumers. It's absolutely a channel to engage CISOs, with 87% saying they use social media to stay informed about the world.

Seeing something on social media may not be the clincher for CISOs when it comes to making decisions, but they are undeniably present and active on these channels.

They are not the most prolific posters, but that doesn't mean there aren't opportunities to influence CISOs.

Firstly, they are signed up to multiple channels. Instagram comes out on top with 77% of CISOs using it. But nearly three quarters are on Twitter, 69% use Facebook, and two thirds are using LinkedIn.

Moreover, they aren't just passive members; more than half of CISOs are reading posts and content, a third are looking to make connections, and a quarter are commenting on other people's posts.

				
Reads content	51%	53%	54%	52%
Publishes content	17%	11%	16%	19%
Searches for connections	33%	35%	37%	38%
Shares content from others	25%	24%	27%	33%
Comments on posts	26%	25%	16%	27%

Do something bold

The purpose of these insights is to help you adopt the right strategy to reach CISOs specifically.

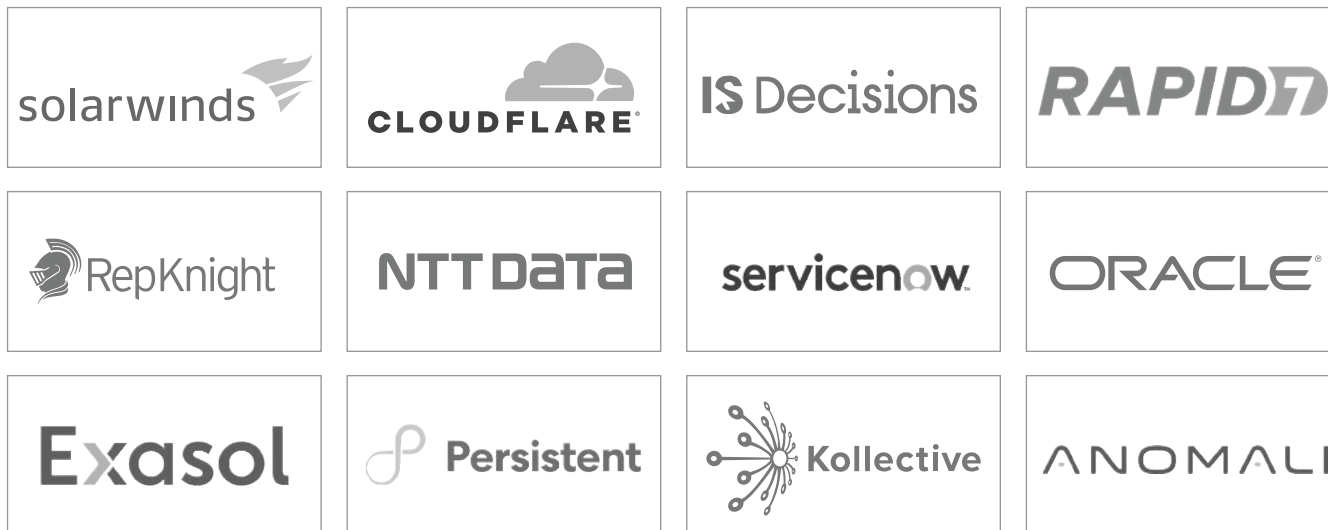
Putting these insights to work doesn't mean doing what you've always done, or what's 'safe' either. It means you can be **BOLD** — in your strategy and your ideas. Great campaigns don't come from following the herd or doing something that any brand could replicate.

That's where Wildfire comes in. Our PR consultants are experts in building effective, creative IT-security campaigns that cut through with CISOs.

From changing the plot of Hollywood blockbusters to holding funerals for software, we put our in-depth insights into action to create campaigns that stand out and deliver.

Check out these examples for yourself on our website:

www.wildfirepr.com/work



wildfirepr.com
+44 20 8408 8000
enquiries@wildfirepr.com

「Think® Bold」

wildfire