Five Cybersecurity PR Mistakes To Avoid In 2023

THE FLYWHEELERS

2023 is upon us.

The success of new marketing and comms plans won't just be defined by looking to the trends ahead (or creating a content plan based on ChatGPT). It also demands honest, constructive reflection.

What worked?

What didn't?

What do we need to do better?

Those are questions marketing and comms teams must ask to inform an even bigger brand boost in 2023. But what happens when we take a step back and look at the wider market?

What were the common PR mistakes cybersecurity companies made in 2022 – and how can you avoid them in 2023?

Ambulance chasing

News hijacking is at the heart of any good cybersecurity PR programme. And if your team isn't actively spotting and jumping on breaking news, I'd ask what they are doing. Because sharing your expertise on the latest hack or vulnerability can act as a great brand credibility boost.

The real question is: what news are they jumping on?

Is it an area where you have authority, relevant insights to add, or something new to share? If not, it may not be a valuable exercise.

Because while ambulance chasing all and any breaches might drive up your coverage volume and Share of Voice, it won't improve your customers' understanding of your offering and how you can help them.

Making it all about hard news

Even when done right, it can't all be about news hijacking. Speaking with a number of business and marketing leaders in cybersecurity companies, many were delighted with the coverage they'd achieved last year with reactive commentary – often in top tier titles. But they still found that comms wasn't moving the needle.

Why? Because while it's great to be a credible commentator in a breaking story, news hijacks rarely offer an opportunity to engage your stakeholders in your point of difference and the problem that you can solve.

Proactive communications - thought leadership, interviews, executive profiles and customer stories - have to balance the reactive to help feed the funnel.

Losing your point of difference

When you are operating in a noisy market, it can be tempting just to shout the loudest.

WE PREVENT RANSOMWARE. WE SECURE THE CLOUD. WE HAVE ZERO TRUST ARCHITECTURE. Great. So do literally hundreds of your competitors. What makes you different?

If there's something genuinely special about your product, what pain point does it solve that your competitors' products don't? What data can you use to exemplify it – proprietary or third-party? And how can you creatively illustrate it?

One of my favourite examples of this was working with a client to highlight the growing risk of steganography – where information is concealed in the pixels of images. We stegged an article written by the publication we were pitching into a "cyber stock image" to demonstrate how undetectable the threat was. This approach meant that the journalist and their audience could see the risk with their own eyes!

Or, if there's something genuinely special about your company and your people (this is particularly key for MSSPs), how are you showing them this? What is your leadership championing? Who are the rising stars that are the future of not just your company, but the industry? Who are your external advocates?

With CISOs and CIOs notoriously sceptical of any marketing fluff, you need to communicate in the clearest terms how you are different and why you are the right investment.

Not speaking to sector challenges

There is no doubt that most industries face very similar cybersecurity threats. Ransomware, DDoS, phishing, Drive-by Download attacks – they are felt across almost all industries. But the frequency with which some sectors are attacked with certain attack vectors differs. The challenges they face in preventing them are also not the same. Nor is the impact that a successful attack can have.

For example, research from Forcepoint this year highlighted the different challenges faced amongst Critical National Infrastructure providers. The survey of CNI cybersecurity professionals highlighted that in the banking sector phishing and IoT-based attacks were perceived to pose the greatest risk, compared to Ransomware, DoS and DDoS in the energy sector.

Speaking directly to the particular challenges that cybersecurity professions in certain industries face – the attacks, the hurdles and the ultimate risk – will help establish your expertise and credibility beyond just another security product vendor.

Forgetting the importance of relationships

There are a lot of security companies out there all fighting for a shrinking pool of media.

In PR, we understand the power of relationships. We spend time networking to make sure that we know the media landscape inside out and are building the right contacts for our clients.

But it's not PRs that journalists ultimately want to speak to. So making a similar investment in building relationships between your business and security leaders with relevant media is key to becoming someone that they not only look forward to hearing from, but proactively seek out the opinion of.

Not every engagement will result in coverage. But like any relationship, it builds credibility and trust. And importantly, it makes your brand memorable when those important stories do come around.

Want to avoid these mistakes in 2023?

There's still time!

Reach out to us at **Hello@TheFlywheelers.com** to hear how we could help you boost your brand awareness, credibility and feed the funnel without falling into these common cybersecurity PR traps.

About the author

Kate Baldwin is the Founder & Managing Director of The Flywheelers. With a decade's experience developing and executing award-winning campaigns, she launched The Flywheelers to help industry disruptors build real momentum against their business and marketing priorities through comms.

Over the course of her career, she has been pivotal in developing narratives and leading the communications programmes for cybersecurity companies, including Darktrace, Forcepoint, McAfee, Thales, Veracode, VMware Security, Worldr and more.

About The Flywheelers

The Flywheelers is a specialist B2B tech communications agency. The team of comms and content marketing specialists has extensive experience storytelling with cybersecurity companies - from pre-seed startups through to some of the industry's most dominant players - across high-impact media relations, owned content, including whitepapers and blogs, and on social media.

Find out more at TheFlywheelers.com