ARE CYBER ATTACK SURGES DUE TO ABSENT SOLUTIONS OR, OVERLOOKED SERVICES?

Introduction

The world of cybersecurity is a vast and complex place, filled with countless threats and concerns. Technology is advancing at a staggering rate. However, as we open the doors for new opportunities and innovations, a new era of cyber-attacks begins to slip through. Cybersecurity companies are needed now more than ever.

So, where are they?

In a study undertaken by Stanford University, 88% of data breaches are caused by an employee mistake.

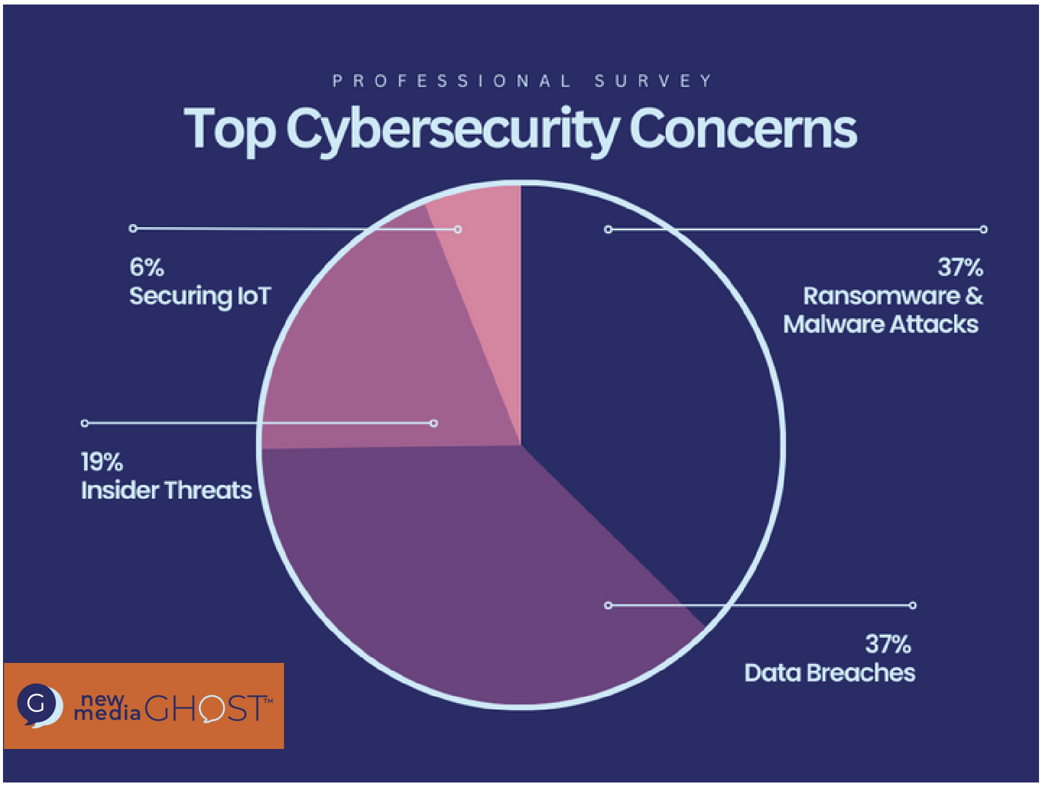
When data breaches are at an all-time high, with over 612 million breached records so far this year, it begs the question of why cybersecurity companies aren't doing more to protect businesses.

At New Media Ghost, we argue that the issue isn't a lack of solutions, but a lack of awareness. Cybersecurity systems can only be put in place if a business actively invests in them. This brings us to the main question we'll be exploring in this white paper.

Are businesses not taking enough initiative or are cybersecurity companies failing to promote their solutions?

Background

Before we delve into who should be taking responsibility, we first need to investigate the main cybersecurity issues businesses should be concerned about. **In a recent survey of 300 cybersecurity professionals**, we gathered data on what they believe to be the top cyber threats they are most concerned about. Firstly it is:



1 Data Breaches & Ransomware/Malware Attacks

When nearly 1 billion emails were exposed last year with almost 236.1 million ransomware attacks occurring globally in just the first half, it comes as no surprise that these two categories were tied as the main concern for cybersecurity professionals garnering 37% each. They dominated the survey taking up **a combined 74% of it**.

On an even more concerning note, the US Department of Justice estimates that as much as 85% of cyber-crimes go unreported, bringing into light the sheer scale of unawareness when it comes to cybersecurity. Most businesses won't even know they've been breached, highlighting how cybersecurity companies need to be pushing the necessity of their services to the attention of SMEs. This also begs the question of how SMEs can find the top cybersecurity companies to help them.

2 Insider Threats

The second most dominant Cybersecurity threat for professionals is insider threats, with 19% of experts believing it to be their top concern. Insider threats originate from within an organisation, such as a current or former employee with legitimate user credentials, where access to the organisation's networks, systems and data is misused and exploited. TechJury has reported that **over 34% of businesses around the globe are affected by insider threats yearly**.

Lockdown Cyber Security stated that “despite millions of phishing emails sent to UK businesses last year, just 4% of UK businesses employ phishing simulation training.” This presents a prime opportunity for cybersecurity firms offering safety awareness training to take a stand and play a crucial role in helping businesses safeguard both their financial stability and reputation.

2,200

Internal Security Breaches Daily

Faced by US Businesses as of May 2023, according to Astra.

3 Securing IoT

Threats concerning the Internet of Things, otherwise known as IoT, accounted for only 6% of the poll. Whilst it doesn’t appear to be the top concern for most professionals, it certainly isn’t one to be taken lightly. When there are nearly 24 billion IoT devices and Operations Units present in the world, it seems like this issue isn’t being taken seriously enough as a staggering 1.51 billion IoT breaches were reported in the first six months of 2022 alone.

98%

Of IoT Traffic Remains Unencrypted

Leaving vast amounts of personal and confidential data exposed, according to G2.

These shocking statistics bring to light how, despite being the main concerns of cybersecurity experts, there seems to be a worrying lack of solutions. However, we need to be asking whether this is really about a lack of solutions or a lack of *awareness.*

> Statistics reveal that human error accounts for 95% of all data breaches. This highlights a clear lack of awareness of cybersecurity solutions within businesses and individuals. So, now this begs the question:
>
> **What are cybersecurity companies doing to promote the value and necessity of their solutions?**

Cyber Professionals: Ignorant or Unaware?

> From the results collected, it is clear that cybersecurity professionals are actually concerned with a number of threats plaguing the digital world. In fact, there are a number of companies specialising in each of these various aspects. So, why are there still so many breaches?

Researching Threats

Despite the efforts to raise awareness, many businesses are still painfully oblivious to the threats that cyber-attacks pose. Statistics show that only 14% of SMEs have a cybersecurity plan in place, exposing the potential for huge losses of funds and resources. It appears that not enough business owners understand the necessity for strong cybersecurity solutions. Whilst those in CISO roles do enforce security policies to protect critical data, they still need to realise that cybersecurity companies are a vital component in the process.

$25,000

Is Lost By SMEs On Average

Due to cyber-attacks and cybersecurity related issues, according to Astra.

Promoting Solutions

Given the multitude of businesses oblivious to the repercussions of a security breach, it's important for cybersecurity firms to actively highlight the value of their offerings. A large portion of SMEs, and even substantial enterprises, fail to recognise these solutions as essential. This mindset requires a shift. It's time for cybersecurity firms to step up and underscore the significance of their services to business decision-makers. Instead of merely concentrating on selling their solutions, firms must prioritise making their audience aware of the underlying issues. Highlighting the potential substantial losses and challenges that SMEs may encounter is crucial in resonating with prospective clients.

As experienced marketers in the cybersecurity field, New Media Ghost has identified a notable gap where cyber businesses struggle to connect with their prospective audiences.

90%

Of Cybersecurity Marketers Don’t Have Enough Time For Content Creation

Despite it generating 3x as many leads than traditional marketing techniques.

What's The Solution?

Now that we've looked into the root of these issues, you might be wondering how both cybersecurity companies and SMEs would go about solving them. Whilst there are a number of practical solutions, we've provided one of the easiest and most effective ways to improve and enhance cybersecurity awareness.

Researching Cybersecurity Companies

How can you expect prospects to reach out for your solutions if they weren't even aware of their issues in the first place? It is crucial to actively promote your solutions and inform your prospects about the threats they are exposed to. If you are uncertain whether your marketing strategies are effectively conveying your company's value, we have created a complimentary quiz tailored for you!

Let's assess your standing from your audience's perspective and determine the level of awareness your customers have regarding your cybersecurity solutions!

Take The Free Questionnaire Now!

You may be concerned that a strong marketing campaign takes a lot of dedicated time and resources, which could be better spent on protecting your clients from cyber-attacks. This is where we come in. The key to crushing cybersecurity threats is raising awareness of them, and that's exactly what we can help you do. Let us at New Media Ghost manage your digital presence, allowing you to communicate with your target audience clearly and effectively, increasing awareness of your cybersecurity solutions.

Conclusion

In conclusion, the issue of a lack of awareness in cybersecurity is one that is multifaceted and shared. Both cybersecurity marketing professionals and leaders of cyber businesses bear the responsibility for this gap. The marketing professionals, for not adequately marketing their services and thereby failing to educate potential clients on the essentiality of these services; and the business leaders, for the lack of awareness of the time and resources required to help their marketers promote their cyber business to their potential client. This lack of awareness and action has a domino effect that impacts not only individual businesses but the entire digital ecosystem because your clients have the right to know you exist so that they can be protected against cyber threats.

It is crucial for cybersecurity businesses to recognise that marketing their services is not just about gaining clients, but about raising awareness and educating businesses on the threats they face. This, in turn, contributes to a safer digital landscape for all. Whether a business has an internal marketing department or not, it is often beneficial to seek external expertise in this area. New Media Ghost can serve as a valuable partner in this endeavour, helping businesses to communicate clearly and effectively with their target audience, and ultimately increasing awareness of their cybersecurity solutions.

In a world where cyber threats are continually evolving, and where human error accounts for a significant percentage of data breaches, it is more important than ever for cybersecurity businesses to step up and take responsibility for educating the business community. By doing so, they not only contribute to a safer digital landscape but also establish themselves as leaders in their field.

As a first step towards bridging this gap, we recommend taking our quick questionnaire. This will help you to assess where your business currently stands in terms of audience awareness and will provide valuable insights into areas for improvement. Remember, the first step towards solving a problem is acknowledging that it exists.

Let us help you take that first step.

Summary of Key Points

Our Poll shows that there is a surge in cyber-attacks and data breaches due to a lack of awareness, not the absence of solutions.

Major threats include Data Breaches, Ransomware/Malware, Insider Threats, and IoT Security. Human error accounts for 95% of breaches.

Cyber Professionals are oblivious and leaders require a mindset shift from selling solutions to raising awareness of underlying issues.

Solution - Active promotion of solutions, informing prospects of threats, and managing digital presence effectively.

In conclusion, we assess the shared responsibility between marketing professionals and business leaders. Marketing is about raising awareness and educating on threats, not just gaining clients. New Media Ghost can be a valuable partner in this effort. Assess current standing and areas for improvement through a quick questionnaire of the call to actions below.

The white paper emphasises the importance of raising awareness about cyber threats, the responsibility of cybersecurity professionals and business leaders in this regard, and the role of companies like New Media Ghost in helping manage digital presence and increase cybersecurity awareness.

Next Steps?

Pass this white paper to your CMO or VP of Marketing to see how we can be a valuable extension to your business and assist their marketing department.

Together, let's take a stand against cyber threats and create a safer digital world for everyone.

Complete the Questionnaire Now