

# CYBER THOUGHTS

## MAN VS AI – OUR PREDICTIONS VS CHATGPT

December 2022

## CYBER THOUGHTS

It's that time of the year; prediction time. Since December is a historically quiet month for venture capital we are going to use this space to make three predictions for 2023, and look at some predictions generated by ChatGPT.

Our Predictions:

- 1. Microsoft runs the board in cybersecurity in 2023.** While Microsoft is already one of the biggest providers of cybersecurity, with over \$15B in annual revenue growing at a rate of 40% a year, they are preparing to trounce their competition using their favorite tactic of bundling. From our November 2022 Cyber Thoughts newsletter:

"[Microsoft] is offering to bundle their endpoint solution, Defender, and offering free data upload to Sentinel from MS products along with customer licenses to Office 365 and the Windows OS. CIOs upgrading to MS E5 licenses are using the cost advantage of these by cutting the security tools that they replace to pay for the new licenses."

We think that CIOs will force CISOs to make the move, and as such Microsoft stands to be the big winner.

- 2. Cybersecurity is the bright spot in a recessionary market.** We think that this one is pretty obvious. Attackers aren't going to let up just because of a recession, and companies will continue to spend on cybersecurity. As attackers continue their move to the SMB market, more and ever smaller companies will be driven to start spending on securing their systems.

In 2022 cybersecurity stocks were down ~22%, according to S&P Kensho Cyber Security Index, while the S&P 500 Information Technology Index was down ~30%. While we aren't public market investors, and can't speak to the vicissitudes of public company multiples, this makes sense to us. We expect that the cybersecurity companies that are public will, on average, grow revenue faster and be more robust than their IT counterparts due to the nature of escalating attacks and the further growth of the industry.

It's not unreasonable that this may be an area where incumbent enterprise security won't be the winner, since their tools generally require expertise to deploy, but again this is an area where Microsoft has a major advantage and will likely reap benefits.

- 3. Seed deals will defy gravity because of supply side issues.** Over the past several years, seed rounds have grown in size not because starting a company has become more expensive, but because seed funds have grown in size. In 2015, most seed rounds were less than \$2M, with the high end of the range being \$4M. Last year, that number had doubled to \$4M with a high of over \$10M.

While valuations are falling at series A and later, we don't believe the size of seed rounds will follow suit. We believe that the \$4M+ seed round is here to stay.

The reason is mostly a supply-side issue. Fund sizes for seed stage investors have grown substantially. Seed investors can no longer get by with writing \$100k-\$500k checks and, instead, are structurally forced to make \$1M+ investments. Because they promised investors that they would do seed stage deals, the size of seed rounds have had to grow. Hence, we think that the new normal is larger seed rounds, potentially requiring further traction from companies, which would also mean the investors are getting a more valuable company for the same valuation. What used to be a seed round will now be labeled pre-seed.

Another way to say this is that seed has morphed into the smaller series A rounds of the prior decade and pre-seed rounds are the seed rounds of that period. It remains to be seen if this new seed round will require the revenue traction of \$1-2M that used to be the series A milestone.

**Now, here is what ChatGPT tells us the future holds.**

Q: Can you give me 3 predictions for the cybersecurity market for next year?

ChatGPT:

It is difficult to make accurate predictions about the cybersecurity market for the coming year, as it is constantly evolving and subject to a wide range of factors. However, here are three potential developments that might occur in the cybersecurity market in the near future:

- 1. Increased demand for cybersecurity solutions:** As more and more organizations and individuals become aware of the importance of protecting their online assets, the demand for cybersecurity solutions is likely to increase. This could lead to the development of new technologies and the growth of existing cybersecurity companies.
- 2. Greater focus on data privacy:** With the increasing amount of personal and sensitive data being shared online, there is likely to be a greater focus on protecting this data and ensuring that it is used in an ethical and responsible manner. This could lead to the development of new technologies and strategies for safeguarding data privacy.
- 3. Increased adoption of artificial intelligence and machine learning:** Artificial intelligence and machine learning have the potential to revolutionize the cybersecurity industry by enabling computers to analyze large amounts of data and identify patterns that may indicate a security threat. As these technologies continue to advance, it is likely that they will be increasingly used in cybersecurity solutions.

The first prediction is about as obvious as a prediction can be. So, while we agree with ChatGPT, we also think this is a cop-out.

The second prediction is one that we've believed in the past, but has never panned out for us. The idea that people will care about privacy makes a ton of sense, but it never actually seems to happen. We happily give up tons of data about ourselves on sites like Facebook and Google in exchange for pictures of cats and curated search results. Perhaps this is the year, but we'd bet against ChatGPT on this one.

The third prediction though does feel like a great answer. Maybe a bit obvious given the AI hype of the past six months, but since ChatGPT is responsible for a lot of that hype, we will give it full credit here.

Hopefully, when we return in a year to review these predictions, we will find that our human predictions have outperformed the AI ones; otherwise, this newsletter will be written by ChatGPT instead of us going forward. ;)

## WHAT WE'RE READING

Here's a curated list of things we found interesting.

### TikTok Spied on Forbes Journalist



The Biden administration recently banned TikTok from government devices, citing its ties to the CCP; here we learn that the company has been spying on journalists as well.

ByteDance confirmed it used TikTok to monitor journalists' physical location using their IP addresses.

[Continue >>](#)

### Here's What To Know About OpenAI's ChatGPT—What It's Disrupting And How To Use It

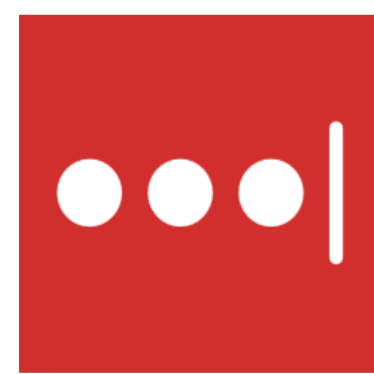


ChatGPT has helped AI come to the masses; the simple interface lets anyone ask questions and get often mind-blowing results. We suggest you create an account and try it for yourself if you haven't already.

OpenAI released ChatGPT, its prototype AI chatbot that has gained a lot of traction among the public for its human-like, detailed answers to inquiries.

[Continue >>](#)

### Yes, It's Time to Ditch LastPass



While we still recommend using a password-manager, LastPass can no longer be trusted with your data. The password manager's most recent data breach is so concerning, users need to take immediate steps to protect themselves.

[Continue >>](#)

## TRANSACTIONS

Deals that caught our eye.

### Proofpoint Buys Deception Tech Startup Illusive Networks



Enterprise security vendor Proofpoint on Monday announced plans to acquire Illusive Networks, a startup that helped pioneer deception technology to help detect data breaches.

[Continue >>](#)

## ABOUT LYTICAL VENTURES

Lytical Ventures is a New York City-based venture firm investing in Corporate Intelligence, comprising cybersecurity, data analytics, and artificial intelligence. Lytical's professionals have decades of experience in direct investing generally and in Corporate Intelligence specifically.