Behind the Markets: Cybersecurity with Aaron Dubin of Team8

Veröffentlicht am 2. Mai 2024

Christopher Gannatti, CFA
Global Head of Research

Wichtige Erkenntnisse

- Geopolitical risks, whether focused on Iran and the Middle East, the Russia/Ukraine conflict, North Korea, or China, are always present, and cyber activities are a big component of them.
- Team8's cyber themes represent the critical areas of potential growth across the cybersecurity ecosystem and help organise company activities within certain focal ecosystems.
- Aaron was able to relate the themes to certain 'current events', like the 'Shift-Left' focus on software supply chain attacks and the importance of marrying application development and cybersecurity at every step of the process.
- Artificial intelligence has been the 'big topic' for the past 16 months, but without cybersecurity advancing alongside it, the world will be open to significant risks of future attacks.

We were excited to speak to Aaron Dubin, VP of Strategy & Business Research at Team8 on the Behind the Markets podcast.

Team8 works with WisdomTree on the WisdomTree Team8 Cybersecurity UCITS Index, which is tracked by the **WisdomTree Cybersecurity UCITS ETF (WCBR)**, before fees and expenses.

By way of background, Team8's cybersecurity expertise helps organise the array of companies providing different cybersecurity solutions to the market. With different megatrends, one of the most important details regarding how that megatrend connects back to the company's future plans. Team8 does this through eight distinct cybersecurity themes that represent the critical areas for growth in the theme as we move forward. Those themes are:

- Cloud Security
- Resilience & Recovery
- Artificial Intelligence (AI) & Smarter Security
- Security of Things
- Perimeterless World
- Data Security

- Shift-Left
- Layer 8

The conversation covered a wide range of topics in cybersecurity, a few of which we summarise in this piece.

1995 in our current ‘AI Moment’

Primarily, people use 1995 to think about where we might be relative to a possible ‘tech bubble’, which we know burst in 2000.

Aaron made an interesting comparison to where we are with cybersecurity of AI today, in the second quarter of 2024, versus where we were with cybersecurity of the internet in 1995. In those early days, there was a significantly higher risk when providing financial information, credit cards, or personal details online. Today, while nothing is perfect, we are a lot more comfortable with those things than we were. Maybe AI will be on a similar path, as we are similarly early in the process at the moment, as many of the large language models with which we are most familiar were initially released with little if any guardrails on how they could be used.

Some of the most interesting and memorable talks on cybersecurity involve experts showing how to take known systems, like ChatGPT, and ‘jailbreak’ them into breaking through the guardrails that have been put in place. Aaron cited one particularly scary example, where we know that AI can be used today in the context of medical imagery, an important diagnostic tool for certain types of cancer. These systems can be tricked into registering a diagnosis opposite to the reality of the situation, showing how thinking of the security of medical systems should always be of the utmost importance.

It takes a village to start a company

Part of the discussion centered on Team8’s activities as a ‘company-builder.’ They have an expression, ' It takes a village to start a company,’ and when we think of cybersecurity and how Team8 operates in the cybersecurity venture space, it starts with their village of 350 Chief Information Security Officers (CISOs) at Fortune 500 companies.

An open dialogue with these professionals uncovers certain unmet needs, and from these unmet needs, sometimes, companies can be founded and built. When we think of the ‘8’ in Team8, it comes back from Unit 8200 of the Israeli military, which is the elite cyber unit of the Israeli Defense Force. Nadav Zafrir, the Co-Founder and Managing Partner of Team8, was the Commander of Unit 8200 during his military career. Many Team8 founders, particularly in the cybersecurity area, have experience serving in this unit.

Connecting current events to Team8’s cyber themes

One of the most interesting parts of our discussion with Aaron regarding the connection between the eight, aforementioned ‘cyber themes’ to current events and headlines that many of us may have seen in different publications.

Linux[1]

Aaron's description of a 'supply chain attack' that was recently thwarted was an important illustration of how today's hackers may be able to access certain systems used by many different customers. Many of us might remember Solar Winds – the issue there was not necessarily any single hack but rather how, from that breach, the hackers were able to access the customers using the Solar Winds system.

In the Linux case, it appears that a Microsoft researcher thwarted the possible attack before the worst possible cases could be realised. It is telling, however, that many developers today are not incentivised to secure the applications they create, and a lot of code is repurposed from various sources. It takes a lot of effort to continually secure and update that code – think about the effort it takes to ensure your smartphone is regularly updated.

The theme 'Shift-Left' refers to how there are efforts to encourage developers to incorporate security earlier in the development process and to secure their code continually. The iPhone was only released in 2007, so we'd note that what we think of as the 'app economy' and 'software-as-a-service' has not been around for that long, in historical terms.

Human error (Layer 8)

The eighth theme on Team8's list – the most recently added – focuses on humans. Even if we might picture popular movies where complex firewalls seem to be breached with ease, we discuss how the vast majority of hacks in the real world do not occur from breaking complex encryptions or doing incredibly technical things – they come from human error.

Aaron noted that the most obvious source of breaches, at least in the second quarter of 2024 from what he is seeing, comes from misconfiguring cloud access points. It's not that the cloud itself is not secure – it is that the humans who are setting up how they access the cloud are making mistakes.

What is 'zero-trust'

It says a lot that many of us might have, by now, heard of 'two-factor authentication.' Simply put, when you are logging into a system and your cell phone generates an additional code, that is an example of this practice at work. Zero-trust, however, is not as commonly used in popular media.

When we think of zero-trust software architecture, one can think of it as constant verification. When people are accessing systems, those systems could be constantly monitoring what they are doing and how they are doing it to determine if those individuals are where they should be and that the system itself remains secure. How this works is similar to how credit card companies use anomaly detection to send out notifications about different transactions that appear 'odd', relative to what the primary account holder usually does. The same principle can apply to accessing a company's network; there are the things that users normally do, and there are possible deviations away from those things that can be flagged and addressed.

Cybersecurity: A megatrend for all seasons

As we write these words in the second quarter of 2024, cybersecurity is no longer an option. Every individual and company needs to have an approach; if they do not, they are taking a huge risk. Of course, when we look company by company, it is never certain which businesses will rise to the top of the heap and provide the best solutions. This is the benefit of our regular dialogue with Team8, in that it helps us to continually understand developments in the cybersecurity space which can evolve quite quickly. Enjoy our most recent discussion with Aaron Dubin, available here.

Sources

[1] Source: Roose, Kevin. “Did One Guy Just Stop a Huge Cyberattack?” New York Times. April 3, 2024.

Important Risks Related to this Article

IMPORTANT INFORMATION

Marketing communications issued in the European Economic Area ("EEA"): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. Past performance is not a reliable indicator of future performance. Any historical performance included in this document may be based on back testing. Back testing is the process of evaluating an investment strategy by applying it to historical data to simulate what the performance of such strategy would have been. Back tested performance is purely hypothetical and is provided in this document solely for informational purposes. Back tested data does not represent actual performance and should not be interpreted as an indication of actual or future performance. The value of any investment may be affected by exchange rate movements. Any decision to invest should be based on the information contained in the appropriate prospectus and affer seeking independent investment, tax and legal advice. These products may not be available in your market or suitable for you. The content of this document does not constitute investment advice nor an offer for sale nor a solicitation of an offer to buy any product or make any investment.

An investment in exchange-traded products ("ETPs") is dependent on the performance of the underlying index, less costs, but it is not expected to match that performance precisely. ETPs involve numerous risks including among others, general market risks relating to the relevant underlying index, credit risks on the provider of index swaps utilised in the ETP, exchange rate risks, interest rate risks, inflationary risks, liquidity risks and legal and regulatory risks.

The information contained in this document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public offering of shares in the United States or any province or territory thereof, where none of the issuers or their products are authorised or registered for distribution and where no prospectus of any of the issuers has been filed with any securities commission or regulatory authority. No document or information in this document should be taken, transmitted or distributed (directly or indirectly) into the United States. None of the issuers, nor any securities issued by them, have been or will be registered under the United States Securities Act of 1933 or the Investment Company Act of 1940 or qualified under any applicable state securities statutes.

This document may contain independent market commentary prepared by WisdomTree based on publicly available information. Although WisdomTree endeavours to ensure the accuracy of the content in this

document, WisdomTree does not warrant or guarantee its accuracy or correctness. Any third party data providers used to source the information in this document make no warranties or representation of any kind relating to such data. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any affiliate, nor any of their respective officers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.

This document may contain forward looking statements including statements regarding our belief or current expectations with regards to the performance of certain assets classes and/or sectors. Forward looking statements are subject to certain risks, uncertainties and assumptions. There can be no assurance that such statements will be accurate and actual results could differ materially from those anticipated in such statements. WisdomTree strongly recommends that you do not place undue reliance on these forward-looking statements.

WisdomTree Issuer ICAV

The products discussed in this document are issued by WisdomTree Issuer ICAV (“WT Issuer”). WT Issuer is an umbrella investment company with variable capital having segregated liability between its funds organised under the laws of Ireland as an Irish Collective Asset-management Vehicle and authorised by the Central Bank of Ireland (“CBI”). WT Issuer is organised as

an Undertaking for Collective Investment in Transferable Securities (“UCITS”) under the laws of Ireland and shall issue a separate class of shares (''Shares”) representing each fund. Investors should read the prospectus of WT Issuer (“WT Prospectus”) before investing and should refer to the section of the WT Prospectus entitled 'Risk Factors' for further details of risks associated with an investment in the Shares.

Notice to Investors in Switzerland – Qualified Investors

This document constitutes an advertisement of the financial product(s) mentioned herein.

The prospectus and the key investor information documents (KIID) are available from WisdomTree's website: **https:** //www.wisdomtree.eu/en-ch/resource-library/prospectus-and-regulatory-reports

Some of the sub-funds referred to in this document may not have been registered with the Swiss Financial Market Supervisory Authority (“FINMA”). In Switzerland, such sub-funds that have not been registered with FINMA shall be distributed exclusively to qualified investors, as defined in the Swiss Federal Act on Collective Investment Schemes or its implementing ordinance (each, as amended from time to time). The representative and paying agent of the sub-funds in Switzerland is Société Générale Paris, Zurich Branch, Talacker 50, PO Box 5070, 8021 Zurich, Switzerland. The prospectus, the key investor information documents (KIID), the articles of association and the annual and semi-annual reports of the sub-funds are available free of charge from the representative and paying agent. As regards distribution in Switzerland, the place of jurisdiction and performance is at the registered seat of the representative and paying agent.

For Investors in France

The information in this document is intended exclusively for professional investors (as defined under the MiFID) investing for their own account and this material may not in any way be distributed to the public. The distribution of the Prospectus and the offering, sale and delivery of Shares in other jurisdictions may be restricted by law. WT Issuer is a UCITS governed by Irish legislation, and approved by the Financial Regulatory as UCITS compliant with European regulations although may not have to comply with the same rules as those applicable to a similar product approved in France. The Fund has been registered for marketing in France by the Financial Markets Authority (Autorité des Marchés Financiers) and may be distributed to investors in France. Copies of all documents (i.e. the Prospectus, the Key Investor Information Document, any supplements or addenda thereto, the latest annual reports and the memorandum of incorporation and articles of association) are available in France, free of charge at the French centralizing agent, Societe Generale at 29,

Boulevard Haussmann, 75009, Paris, France. Any subscription for Shares of the Fund will be made on the basis of the terms of the prospectus and any supplements or addenda thereto.

For Investors in Malta

This document does not constitute or form part of any offer or invitation to the public to subscribe for or purchase shares in the Fund and shall not be construed as such and no person other than the person to whom this document has been addressed or delivered shall be eligible to subscribe for or purchase shares in the Fund. Shares in the Fund will not in any event be marketed to the public in Malta without the prior authorisation of the Maltese Financial Services Authority.

For Investors in Monaco

This communication is only intended for duly registered banks and/or licensed portfolio management companies in Monaco. This communication must not be sent to the public in Monaco.