CYBERSECURITY: The Megatrend for All Seasons

Introduction by: **Christopher Gannatti,** CFA, Global Head of Research, WisdomTree
Theme discussions and quotes written and coordinated by: **Team8**

At WisdomTree, we manage strategies across an array of different megatrends, and one that always stands out to us—particularly by way of stories—is cybersecurity. Think of it this way: If there is a company or a person out there looking to save money, how much bang for the buck might there be in CUTTING cybersecurity spending? Many of us would look at that and think that the risk is not worth the potential reward.

Attackers are always seeking an advantage, so the demand to defend, in our view, should remain healthy across all economic environments. Unfortunately, they may not always lead to positive investment returns across specific stocks over different periods. Sometimes the picture ends up like 2022, when a macroeconomic force—in this case central banks shifting interest rates higher quite quickly—causes an apparent divergence between the investment returns of the public market stocks and the apparent need for cybersecurity services. Similarly, sometimes the picture ends up looking like 2023, when the market starts looking forward to a time when interest rates may ultimately fall, and the market return of publicly listed cybersecurity stocks can be quite high.

The juxtaposition of these two distinct years reminds us that while cyber attackers are always attacking and cybersecurity defenders are always defending, the public market equity returns can be quite volatile.

In our opinion, thinking about the importance of cybersecurity and organizing the space in a way that helps to make it appear more digestible could be an approach that allows investors to connect more with the long-term cybersecurity megatrend and weather any shorter-term equity volatility.

We are fortunate to be able to work with Team8, a venture firm with an exceptional level of experience in analyzing trends within cybersecurity. In this article, we are able to benefit from the perspective of Nadav Zafrir and Admiral Mike Rogers. Nadav Zafrir served as Commander of Unit 8200, Israel's elite military technology unit, prior to co-founding Team8. Admiral Rogers culminated his distinguished U.S. Navy career with a four-year tour as Commander, U.S. Cyber Command, and Director, National Security Agency.

Together, their experience and accomplishments bring the highest level of perspective from two of the most capable countries within the cyber space.

GEOPOLITICAL PRESSURES

Whether one thinks of Russia's invasion of Ukraine, ongoing conflict in the Middle East or the well-known tensions regarding Taiwan, the geopolitical need to pay attention to cyber defenses at the nation-state level never goes away. We believe that any time there is conflict of any type, it will be important to think of the potential for both physical and cyber attacks.

Nadav Zafrir: *Geopolitical tensions are escalating, and cyber threats are being leveraged as a tool of statecraft. As nations continue to compete for power and influence, cybercrime has become a valuable asset in the modern arsenal. The recent Russia-Ukraine conflict illustrates how cyber operations can be used to support physical combat and achieve strategic objectives.*

With sanctions now targeting not only financial assets but also knowledge, we can expect to see an increase in nation-state attacks aimed at stealing secrets and acquiring funds. This underscores the urgent need for global collaboration to address cybersecurity challenges and protect the most vulnerable countries, particularly those at or below the poverty line.

GLOBAL ECONOMY AND BUDGETS

One of the biggest ongoing discussions regards the health of the global economy and whether central banks, in their battle against inflation, have engineered the so-called 'goldilocks' soft-landing. A recession has been long-discussed, but as we write these words, we haven't seen it. While we don't believe that attackers will take this into account and lower their efforts, it's important to consider how this economic dynamic may contribute to what we are seeing in the activities and fundamentals of different cybersecurity companies.

Nadav Zafrir: *Due to the current global macroeconomic situation, corporate budgets for cybersecurity are becoming constrained. As a result, it may be more difficult for CISOs to get certain budgetary requests approved. Budgets may not necessarily go down, but the growth may slow down dramatically, or, in some cases, remain flat. In response, cyber practitioners will need to focus on leveraging tools and technologies that enable them to prioritize critical security issues and create more efficiency through automation, etc.*

At the same time, cyber vendors will need to demonstrate real, measurable ROI in order to justify their place in the customer's toolkit. In the last several decades, the global economy has continued to become more efficient based on competitive advantages, which is typically a good thing for everyone…

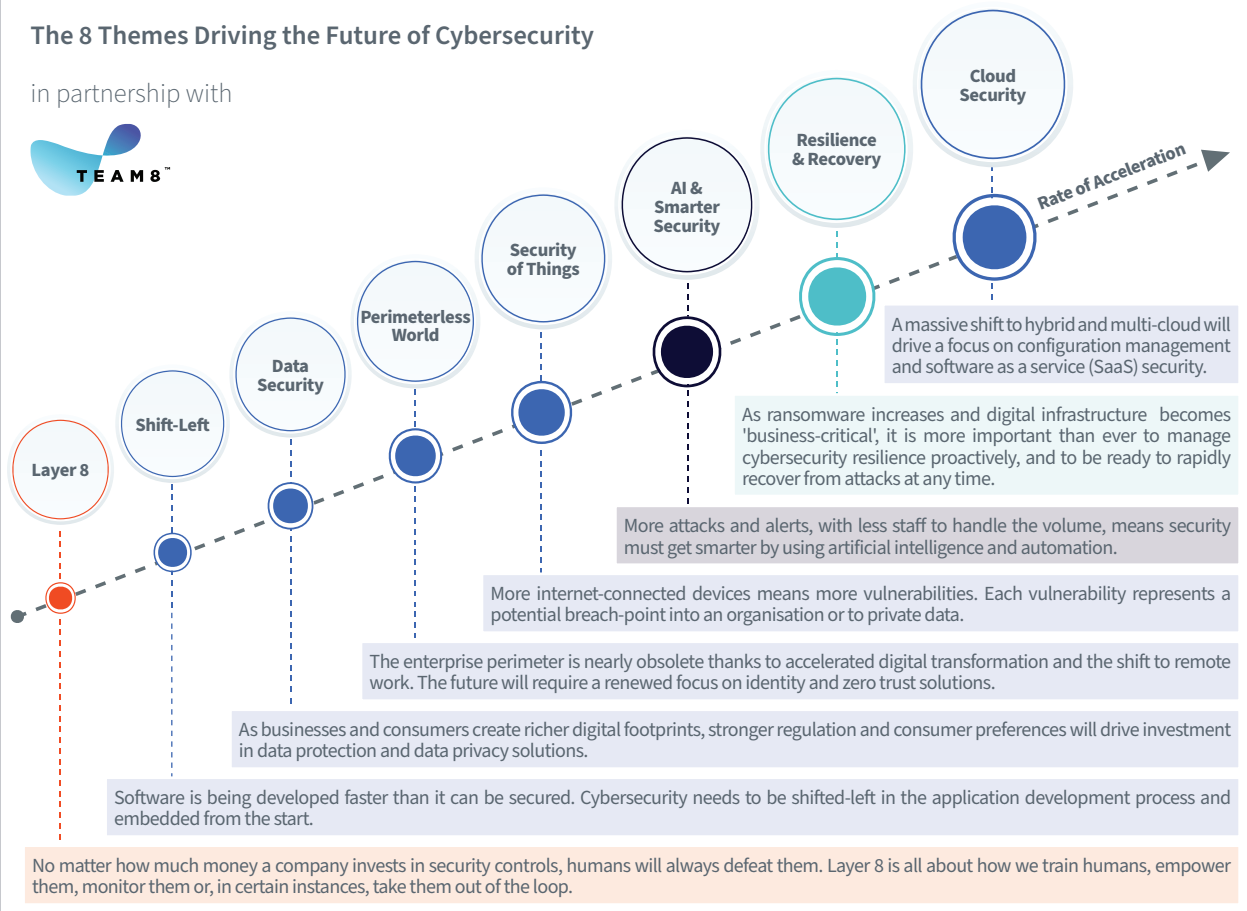
Unfortunately, this may not be where we're heading. Specifically, there are concerns around topics such as global prices for raw materials and energy, as well as the interdependence and independence of the global supply chain, among others.

ORGANIZING THE CYBERSECURITY LANDSCAPE: FROM GREATER STRUCTURE, WE MAY ACQUIRE GREATER UNDERSTANDING

While a simplistic take on cybersecurity may mean "protecting systems from hackers," it's important to recognize that there is a lot more than that going on across the different companies. Team8 and WisdomTree collaborated to create a series of eight investment themes within the cybersecurity space. This is helpful in placing the different types of activities done at the company level into better context to see how different trends are evolving within the broader megatrend.

Figure 1 is a representation of this structure.

Figure 1: Team8 and WisdomTree's Conceptualization of Eight Distinct Cybersecurity Themes



Source: Team 8 and WisdomTree, 2023.

From Figure 1, we can then look at how Nadav Zafrir and Admiral Rogers would speak about each of these different topics, given their backgrounds and expertise in the topic.

THEME 1 OF 8: CLOUD SECURITY

Nadav Zafrir: *As we navigate the accelerating cloud migration, we must recognize that while it presents new security challenges due to its flexibility, it also offers unique security opportunities. Data moves to new partners and services, and the network is flatter and more discoverable for attackers. However, everything is visible, and we have a deeper insight into our systems and what happens in them than ever before.*

With the upcoming power of AI, moving to the cloud will become not only a necessity but an imperative for leading organizations. In the multi-cloud plus SaaS world we live in, with cloud operators solving part of the equation and cloud-native services becoming better and better, operating securely in the cloud is core to almost all businesses.

Admiral Rogers: *As targets (companies) begin pivoting to shifting large chunks of their data to the cloud, you're going to see a heavy focus from nation-state actors on cloud data concentrations.*

THEME 2 OF 8: RESILIENCE AND RECOVERY

Nadav Zafrir: *Ransomware is a sophisticated and financially motivated attack that has become more prevalent in recent years, with attackers using increasingly sophisticated methods to infiltrate organizational networks, especially, as in many cases, they are supported today by governments. As a result, organizations must be proactive in their approach to security, recognizing that it is not a matter of if but rather when they will face a ransomware attack.*

To effectively combat this threat, organizations are shifting their focus from solely trying to prevent attacks to also preparing for the inevitability of a successful attack. This means building a comprehensive security strategy that includes not just technical controls to detect and prevent attacks but also well-defined policies, procedures and training to allow continued operation and rapid recovery. By adopting this approach, organizations can increase their resilience in the face of an attack and ensure a speedy recovery while maintaining critical business operations.

Admiral Rogers: *Ransomware is going to continue to be significant in particular sectors more than others, e.g., critical infrastructure/healthcare, etc. The outcome is a focus on "resilience, resilience, resilience," which will continue to be of more and more importance. This will be exacerbated, in particular, if budgets decline and there is a shortfall of people, as businesses will be looking for efficiency wherever they can find it.*

While ransomware has traditionally been about access, we're also going to see an increase in the "embarrassment factor" to get people to pay more in ransom. Though most companies won't acknowledge it, the number of companies paying the ransom is slowly decreasing. What's the criminal response? Ransomware threat actors need to figure out what other motivators will drive the company to pay, e.g., public embarrassment and reputational risk/damage.

THEME 3 OF 8: AI & SMARTER SECURITY

Nadav Zafrir: *In today's fast-paced and complex threat landscape, we have more services and applications than ever before, yet we don't have many more security professionals to protect them. Meanwhile, attacks have become faster and more sophisticated, making it increasingly difficult for organizations to keep up.*

In response, organizations are now demanding smarter security tools that integrate with other technologies, have APIs for customization and provide intelligent recommendations. AI and smarter security also involves using advanced analytics and threat intelligence to identify and respond to potential security threats in a timely and effective manner. By focusing on what is truly important and investing in the right security technologies and practices, organizations can improve their security posture and reduce the risk of cyberattacks.

This trend toward AI and smarter security is only going to accelerate in the coming years. As we navigate the increased complexity, we must leverage new technologies like AI to help us stay ahead of the curve.

Admiral Rogers: *One of the dynamics I see for CISOs going forward is that most CISOs have broadly enjoyed 5-7 years of continual growth—including annual increases in budget and manpower. However, today there are tons of businesses dealing with a potential recession and a tough economic environment. People are getting laid off left and right…*

Going forward, some CEOs may say continual growth in cyber isn't sustainable and that they can't just keep giving CISOs 15% budget increases year after year. We will have to push ourselves to ask, "What does a more efficient, more resource-constrained model look like?" This is where AI and smarter security comes in.

THEME 4 OF 8: SECURITY OF THINGS

Nadav Zafrir: *As the number of connected devices continues to skyrocket, these devices are also becoming increasingly integrated into our lives and, in many cases, have the ability to affect the physical space around us.*

While the value that connected devices bring is clear, they can also be a source of exposure to new and dangerous attack vectors. As such, building scalable security for these devices is of critical importance, particularly for emerging technologies like drones, connected cars, connected health care devices, smart factors and more—all of which can affect our physical world and put lives at risk.

To achieve this, organizations and vendors must develop security strategies and tools that account for the unique risks and challenges presented by the Security of Things. This requires collaboration between manufacturers, regulators and security experts to create standards, frameworks and best practices for securing these devices throughout their entire lifecycle.

Admiral Rogers: *I expect a greater focus on OT and the internet of things (IoT), specifically on functionality, not just data. Look for actors to approach critical infrastructure in a deeper analytical way, i.e., it will no longer be "Let's go after water company X. Let's see if we can get into their network."*

Rather, attackers will look at their targets more holistically, evaluating the network, operating structure, remote access, vulnerabilities in basic and embedded systems, supply chain, etc., to identify the most effective path to achieve their goal. *Rather, attackers will look at their targets more holistically, evaluating the network, operating structure, remote access, vulnerabilities in basic and embedded systems, supply chain, etc., to identify the most effective path to achieve their goal.*

THEME 5 OF 8: PERIMETERLESS WORLD

Nadav Zafrir: *In the modern, cloud-driven and work-from-anywhere world, the classical network perimeter has evaporated. The COVID-19 pandemic and widespread remote work have accelerated this trend, making it clear that our technology estates no longer have a clear boundary.*

With the disappearance of the traditional perimeter, identity is now our perimeter. Users, permissions and endpoints have become the new focus of security, and managing them intelligently is now key to protecting our organizations.

Organizations must adopt solutions that provide visibility and control over user identities, including access control, authentication and privilege management, which are integrated across the cloud, on-prem and in the field. Only then can we establish trust in a world where boundaries have disappeared and ensure that our assets and information are secure while interconnected.

THEME 6 OF 8: DATA SECURITY

Admiral Rogers: *Historically, Americans have held the view that the federal government should minimize its role. Therefore, when it comes to data privacy regulation, in the absence of broad federal legislation, the states have had to step in to fill the void. If you're a large company that works across many domestic geographies, you can't build a solution with 50 different privacy requirements.*

THEME 7 OF 8: SHIFT LEFT

Nadav Zafrir: *As we continue to write more code than ever before, adding security to our software development process is becoming increasingly critical. This means shifting security practices earlier in the development process, or "Shifting Left."*

With the widespread use of open-source software, which forms the foundation of many modern software applications, and with the emergence of low-code and no-code developments, we are rapidly approaching a point where everyone in an organization will be developing and using code.

As such, it's imperative that we ensure all members of the organization have a solid understanding of secure coding practice and that security is built into the software development process from the very beginning.

By embracing a Shift-Left approach to security, we can reduce the risk of vulnerabilities, protect our assets and information and ensure that our software is secure, reliable and resilient.

Admiral Rogers: *The supply chain has become really interesting, and we're seeing more and more attention and focus on this. It started initially with private companies working with the government and there may be a push to expand U.S. supply chain legislation beyond this.*

THEME 8 OF 8: LAYER 8

Nadav Zafrir: *In the world of cybersecurity, the human element is both a critical asset and a significant risk factor. Many recent attacks have targeted humans in ever more sophisticated ways beyond spear-fishing, which is very prevalent today. To address this challenge, we must focus on Layer 8—the human layer—and build tools that empower people to make better security decisions.*

Improving the usability of security tools and making them intuitive for non-technical users is an important frontier. By enabling people to interact with technology securely and efficiently, we can reduce the likelihood of human error leading to security breaches.

At the same time, educating people on best practices and equipping them with the tools and knowledge to make informed decisions is an opportunity to strengthen our organization's security posture. By providing employees with the right training and resources, we can turn them into an asset in the fight against cyber threats.

CONCLUSION: TRACKING THE THEMES ALLOWS US TO TRACK THE ONGOING EVOLUTION OF CYBERSECURITY

One of the most difficult aspects of megatrend investing regards the measurement of progress. Megatrends can be quiet for long periods, and then suddenly, then can splash across almost every headline—just look at AI and ChatGPT over the past couple of years. The different themes allow us to categorize company activities and therefore track the different progress being made across them. They also help in finding new, public company opportunities that may best represent the space.

For those investors interesting in a specific investment strategy that includes these themes as part of the constituent selection process, the WisdomTree Cybersecurity Fund (Ticker: WCBR) may be of particular interest.

Important Information From Team8

This Cybersecurity: The Megatrend for All Seasons Report represents the opinions of Team8 Labs Inc. ("Team8") and is for informational purposes only. You should not treat any opinion expressed by Team8 as a specific inducement to make an investment in any security but only as an expression of Team8's opinions. Team8's statements and opinions are subject to change without notice. Team8 is not registered as an investment adviser advisor under the Investment Advisers Act of 1940, as amended (the "Advisers Act"), and relies upon the "publishers' exclusion" from the definition of investment adviser under Section 202(a)(11) of the Advisers Act. As such, the information contained in this Team8 Cybersecurity: The Megatrend for All Seasons Report does not take into account any particular investment objectives, financial situation or needs and is not intended to be, and should not be construed in any manner whatsoever as, personalized investment advice. The information in this Team8 Cybersecurity: The Megatrend for All Seasons Report is provided for informational and discussion purposes only and is not intended to be, and shall not be regarded or construed as, a recommendation for a transaction or investment or financial, tax, investment or other advice of any kind by Team8. You should determine on your own whether you agree with the information contained in this Team8 Cybersecurity: The Megatrend for All Seasons Report. Certain of the securities referenced in this Team8 Cybersecurity: The Megatrend for All Seasons Report may currently, or from time to time, be constituents of an index developed and maintained by WisdomTree Investments, Inc., using data provided by Team8, which has been or will be licensed for a fee to one or more investment funds. In addition, certain officers or employees of Team8 or funds or other persons or entities affiliated or associated with Team8 may hold shares of, be officers or directors of, or otherwise be associated with some or all of the issuers of the securities referenced in this Team8 Cybersecurity: The Megatrend for All Seasons Report or included in such index. Team8 expressly disclaims all liability with respect to any act or omission taken based on, and makes no warranty or representation regarding, any of the information included in this Team8 Cybersecurity: The Megatrend for All Seasons Report.

Important Information From WisdomTree

This material has been written by third parties not affiliated with WisdomTree or any of its affiliates. No information contained in the material has been endorsed or approved by WisdomTree, and WisdomTree is not responsible for the content. No information accessed through this material constitutes a recommendation by WisdomTree to buy, sell or hold any security, financial product or instrument discussed therein. This information neither is nor should be construed as an opinion regarding the nature, potential, value, suitability or profitability of any particular investment or investment strategy, and you shall be fully responsible for any investment decisions you make, and such decisions will be based solely on your evaluation of your financial circumstances, investment objectives, risk tolerance and liquidity needs.

Investors should carefully consider the investment objectives, risks, charges and expenses of the Fund before investing. To obtain a prospectus, or summary prospectus, containing this and other important information, please call 866.909.9473, or visit WisdomTree.com/investments to view or download a prospectus. Investors should read the prospectus carefully before investing.

There are risks associated with investing, including the possible loss of principal. The Fund invests in cybersecurity companies, which generate a meaningful part of their revenue from security protocols that prevent intrusion and attacks on systems, networks, applications, computers and mobile devices. Cybersecurity companies are particularly vulnerable to rapid changes in technology, rapid obsolescence of products and services, the loss of patent, copyright and trademark protections, government regulation and competition, both domestically and internationally. Cybersecurity company stocks, especially those which are internet-related, have experienced extreme price and volume fluctuations in the past that have often been unrelated to their operating performance. These companies may also be smaller and less experienced, with limited product or service lines, markets or financial resources and fewer experienced management or marketing personnel. The Fund invests in the securities included in, or representative of, its Index regardless of their investment merit, and the Fund does not attempt to outperform its Index or take defensive positions in declining markets. The composition of the Index is heavily dependent on quantitative and qualitative information and data from one or more third parties, and the Index may not perform as intended. Please read the Fund's prospectus for specific details regarding the Fund's risk profile.

WisdomTree Funds are distributed by Foreside Fund Services, LLC. Foreside Fund Services, LLC is not affiliated with or endorsed by WisdomTree LLC or Team8.