A military perspective on cybersecurity (Part 2)

Published 18 May 2023

Christopher Gannatti, CFA
Global Head of Research

Team8
Global venture group

In the first blog of this two-part series, we introduced Nadav Zafrir (who served as Commander of Unit 8200, Israel's elite military technology unit, prior to co-founding Team 8) and Admiral Mike Rogers (who culminated his distinguished US Navy career with a four-year tour as Commander, US Cyber Command, and Director, National Security Agency) as they shared their expert views on the first four of our eight cybersecurity themes for 2023. In Part 2, we hear from these military experts again as they turn their attention to the remaining four themes.

Theme 5: 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 organisations.

Organisations 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-premise 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.

Admiral Rogers: For me, 2022 was all about trying to understand what the new normal looked like in terms of remote/hybrid workforces and the new perimeterless world in which we live. We're now in a position where COVID-19 is something that is sustained without major aperiodic spikes like we used to have. And with it, the distributed work model has become very much the norm. Going forward, the 'hybrid dynamic' will be the focus.

Theme 6: Data security

Admiral Rogers: Historically, Americans have held the view that the federal government should minimise 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.

Thus, in 2023, we must carefully consider what the US regulatory framework should be for data protection and privacy. This is further complicated by the fact that right now, in the US Congress, there is a strong pushback against big tech companies and social media. I expect they'll spend the next few months continuing to debate these topics and, in the fall, we might see a framework of new draft legislation in the data privacy field.

Theme 7: 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 organisation will be developing and using code.

As such, it's imperative that we ensure all members of the organisation 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. However, in 2023, there may be a push to expand US supply chain legislation beyond this.

Theme 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-phishing, 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 organisation'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, they can splash across almost every headline—just look at AI and ChatGPT recently. The different themes allow us to categorise 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.

Related blogs

+ A military perspective on cybersecurity (Part 1)

+ Cybersecurity should remain a top focus in 2023

+ Introducing our newest cybersecurity theme: Layer 8 - The Human Factor

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. The information contained in this document is for your general information only and is neither an offer for sale nor a solicitation of an offer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and affer seeking independent investment, tax and legal advice.

The application of regulations and tax laws can offen lead to a number of different interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and affer seeking independent investment, tax and legal advice.

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 or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. 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.