A military perspective on cybersecurity (Part 1)

Published 10 May 2023

Christopher Gannatti, CFA
Global Head of Research

Team8
Global venture group

While a simplistic take on cybersecurity may mean ‘protecting systems from hackers’, it’s important to recognise that there is a lot more than that going on. Team8 (a venture firm with an exceptional level of experience in analysing trends in cybersecurity) and WisdomTree have collaborated to create a series of eight investment themes within the cybersecurity space.

In this two-part blog series, 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 US Navy career with a four-year tour as Commander, US Cyber Command, and Director, National Security Agency. Together, their experience and accomplishments bring the highest level of perspective from two of the most powerful countries in cybersecurity – let’s unwrap their views on the first four of our eight cybersecurity themes.

Theme 1: Cloud security

Nadav Zafrir: As we navigate the accelerating cloud migration, we must recognise 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 artificial intelligence (AI), moving to the cloud will become not only a necessity but imperative for leading organisations. In the multi-cloud plus software-as-a-service (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: 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 organisational networks, especially, as in many cases, they are supported today by governments. As a result,

organisations must be proactive in their approach to security, recognising that it is not a matter of if but rather when they will face a ransomware attack.

To effectively combat this threat, organisations 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, organisations 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, for example, critical infrastructure/healthcare etc. The outcome is a focus on "resilience, resilience, resilience," which will continue to be of more and more importance in 2023. 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, for example, public embarrassment and reputational risk/damage.

Theme 3: 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 organisations to keep up.

In response, organisations are now demanding smarter security tools that integrate with other technologies, have application programming interfaces (APIs) for customisation, and provide intelligent recommendations. 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, organisations can improve their security posture and reduce the risk of cyberattacks.

This trend toward 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 Chief Information Security Officers (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 smarter security comes in.

Theme 4: 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 factories and more—all of which can affect our physical world and put lives at risk.

To achieve this, organisations 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 operational technology (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, that is, it will no longer be "Let's go after water company X. Let's see if I 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.

Stay tuned for Part 2 where we will cover the remaining 4 themes: permiterless world, data security, shift-left, and our newest theme Layer 8.

Related blogs

+ 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.