Eight essential elements of cybersecurity

Published 15 April 2024

Mobeen Tahir
Director, Macroeconomics and Thematic Research

Key Takeaways

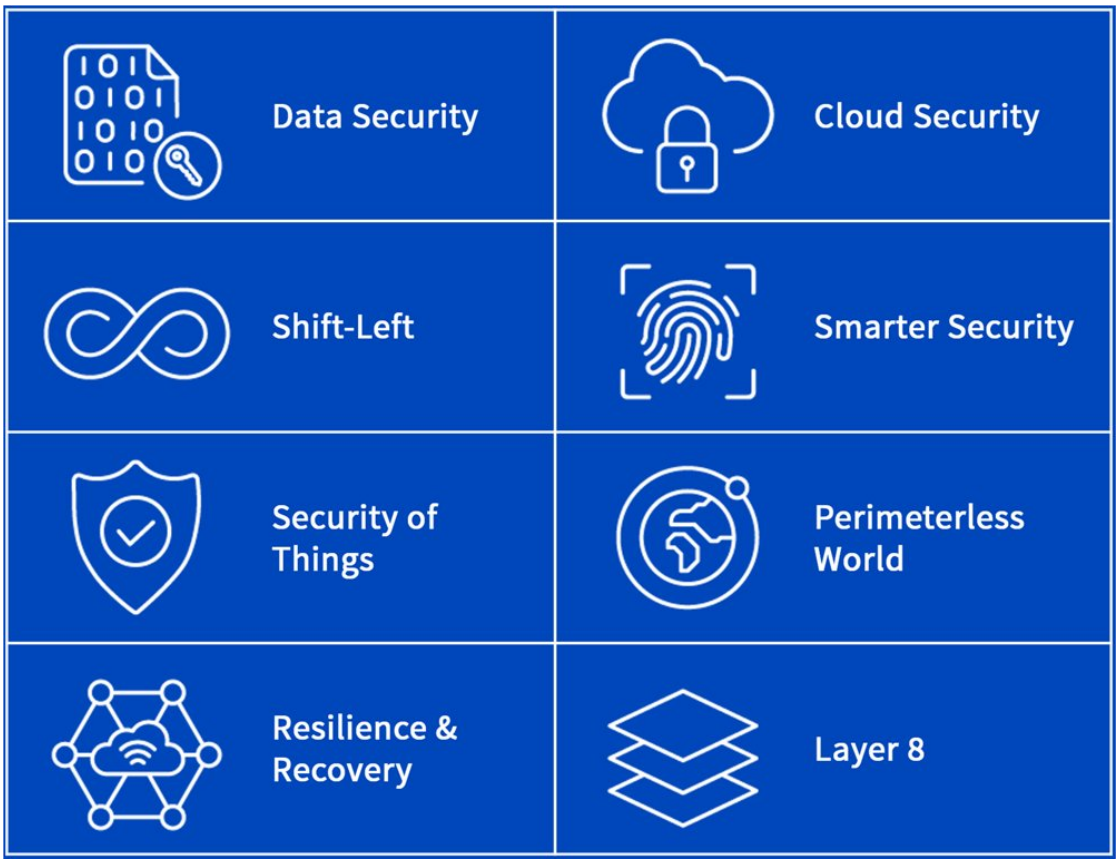
- Cybersecurity risks are on the rise as organisations adopt digital tools.
- From securing data to devices and training people, cybersecurity has many facets.
- Companies with a broad focus across multiple areas of cybersecurity potentially stand a better chance of enduring in a rapidly evolving industry.

On 19 February, the Financial Times reported[1] that North Korean cyber criminals were turning to artificial intelligence (AI) to steal funds and cutting-edge technologies from victims around the world. The report stated how hackers targeted global defence, cyber security, and crypto companies by tricking people on popular platforms like LinkedIn. It also stated that ChatGPT developer OpenAI and its investor Microsoft had also confirmed that bad actors were using their AI services for malicious cyber activities.

Generative AI tools have lowered the bar for people to do more technically sophisticated things with relatively basic skills. Large language models allow users to communicate with the computer in a language like English and let the model translate their commands to write programmes. Unfortunately, technology can also empower bad actors to do unlawful things more easily. This is why cybersecurity must become smarter and seal all potential vulnerabilities before criminals exploit them.

WisdomTree has partnered with venture group Team8 to identify eight distinct cybersecurity areas that are essential in a world with ever-increasing risks.

For cybersecurity to be thorough it needs to be holistic



Source: WisdomTree, Team8, 2024.

Data Security

It is estimated that the world produces 328 million terabytes of data every single day. One terabyte is 1000 gigabytes. In other words, the world is producing a lot of data. Moreover, the world is producing data faster than ever. It is also estimated that 90% of the world's data was generated in the last two years alone[2].

IBM states that the average data breach cost in 2023 was USD4.45 million, a 15% increase over three years[3]. With the world producing more data than ever, protecting that data is paramount. This is what data security aims to achieve.

Cloud Security

All this data being produced means more storage in the cloud. According to one report[4], approximately 60% of all corporate data is stored in the cloud, up from just 30% in 2015. Moreover, 89% of companies use a multi-cloud approach, a term referring to a company using at least two cloud-based applications.

And unfortunately, malicious actors are fully aware of this. In 2023, there was a 110% increase in cloud-conscious cases[5]. This means that cyber adversaries are increasingly looking to attack their targets via cloud-based applications. Securing the cloud is, therefore, a critical theme in cybersecurity.

Shift-Left

Securing the cloud or any other application cannot be an afterthought. Shifting left refers to the idea of integrating cybersecurity at the point when the software is being developed. The opposite of this would be to keep cybersecurity right and rely on generic solutions from third-party providers.

Shifting cybersecurity left allows developers to critically evaluate vulnerabilities within the software to ensure all necessary guardrails are in place when the software is being created. This can reduce costs and expedite delivery as there will likely be fewer problems once the software has been introduced to users.

Smarter security

Generative AI has lowered the bar for becoming a bad actor. It is now easier to create malicious code, like that used in a polymorphic attack in which the cyber-attack changes code, content, and structure to avoid being detected by security systems. Such a code comes back stronger if it gets locked out by a company's security.

Tackling such threats requires automation. Smarter security includes automation tools that can monitor networks for potential threats. This is where AI tools that learn, adapt, and evolve play a crucial role in providing security.

Security of things

The Internet of Things (IoT) refers to devices that are connected to the internet. Laptops and mobile phones are obvious examples but now, increasingly, cars, watches, digital assistants, TVs, dishwashers, and so forth, all belong to the IoT world. It is estimated that there are currently 17 billion IoT devices in the world, and this number could double by 2030[6].

Clearly, our devices need to be protected as they all provide attackers with points of entry for gaining access to our networks and data. The security of things, therefore, is the idea of protecting this growing number of connected devices from potential threats.

Perimeterless world

The so-called attack surface has grown, with organisations having a more significant number of remote workers since the COVID-19 pandemic. This attack surface refers to the sum of vulnerabilities that hackers can exploit to access an organisation's network or sensitive data. Compared to the past, where workers may have been confined within a perimeter, attackers now have more potential entry points.

In a perimeterless world, organisations need more sophisticated tools for protecting themselves. This includes two-factor authentication and biometrics for users to log in to their company network and applications.

Resilience & recovery

In May 2017, the WannaCry ransomware attack cost the UK's National Health Service £92m through services lost and IT costs. Even more importantly, 19,000 appointments were cancelled as more than 80 hospital trusts and 8% of GP practices were disrupted[7].

According to Team8, cybersecurity cannot afford to stop at 'identify, protect, detect, and respond' but must also include the capability for rapid recovery from degradation, disruption, or denial of access to an organisation's network or data. The cost of not being able to do so can be catastrophic.

Layer 8

An organisation may have the most powerful cybersecurity tools to protect itself. But, if the humans aren't trained and equipped to handle risks, the guardrails may disintegrate like a house of cards. Layer 8, therefore, is the human factor.

According to CrowdStrike, 75% of attacks in 2023 were malware-free, up from 40% in 2019. This means that attackers are relying less on malware attacks delivered via phishing emails and using more sophisticated methods like social engineering, which are intended to deceive humans. Thus, empowering people to better manage cybersecurity risks can be the bedrock of all other measures.

Conclusion

Cybersecurity is not optional. Its importance becomes all too apparent when a successful attack takes place. But by then it may be too late to prevent significant damage. A cybersecurity framework that takes a holistic approach to these eight essential elements can give organisations the best chance of avoiding undesirable outcomes.

Sources

[1] https://www.ft.com/content/728611e8-dce2-449d-bb65-cff11ac2a5bb
[2] Sourced from explodingtopics.com as of December 2023 which quotes Statista as the source of information. Explodingtopics.com/blog/data-generated-per-day
[3] IBM's Cost of a Data Breach 2023 report
[4] Sourced from explodingtopics.com as of November 2023 which quotes Thales Group as the sources of information. Explodingtopics.com/blog/corporate-cloud-data
[5] CrowdStrike 2024 Global Threat Report.
[6] Explodingtopics.com as of February 2024 which quotes Transforma Insights as the source of information. Explodingtopics.com/blog/number-of-iot-devices
[7] National Health Executive, October 2018. GP refers to general practitioner.

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.