A Special Cyber Edition: Celebrating a Decade of the L&G Cyber Security UCITS ETF

October 2025

Ilaria Sangalli, *Index Research Lead*

Introduction

This article marks a special milestone: the 10-year anniversary of the L&G Cyber Security UCITS ETF* (London: ISPY/USPY), which directly tracks the ISE Cyber Security UCITS™ Index (HUR™). A decade-long journey of tracking the evolution, performance, and strategic relevance of cybersecurity in global markets.

Since September 2015, when the L&G Cyber Security UCITS ETF began tracking the index, HUR has delivered a total return of +306% (15% annualised)[1], offering investors a clear path to participate in the long-term growth of cybersecurity through a liquid and diversified vehicle. For further details, please refer to Part 3, page 13.

Over the past 10 years, the cyber landscape has undergone a profound transformation. What began as a niche concern has become a central pillar of digital resilience, innovation, and investment. In this special edition, we take a moment to reflect on this evolution, year by year, highlighting the key shifts, threats, and breakthroughs that have shaped the industry.

If the first half of the cyber story is defined by urgency and exposure, the second is shaped by opportunity. From explosive market growth to its increasing role in capital markets, cybersecurity has become a dynamic force in shaping the future of businesses.

Finally, we turn our focus to the HUR Index itself. Over the past decade, it has delivered notable performance, underpinned by strong fundamentals. This deep dive will showcase how the index has captured the essence of the cyber opportunity and why it remains a compelling lens through which to view the next chapter of digital security.

Part 1 - A decade of transformation: the evolution of cybersecurity

20 years ago, cybersecurity was largely seen as a technical safeguard, a necessary but often reactive function focused on firewalls, antivirus software, and patch management. Fast forward to today, and it has become a strategic imperative, a board-level concern, and a dynamic investment frontier.

*** Where L&G Cyber Security UCITS ETF is mentioned, please refer to the appendix**

[1] Price return of +264%. From September 28, 2015 until September 28, 2025. Past performance is not a guide to the future.

The past decade has witnessed an important shift in the cyber landscape. This evolution was catalysed by a series of high-profile breaches, most notably those involving Yahoo[2] and Equifax[3], which exposed the vast scale of digital vulnerabilities and the costly consequences of inadequate cyber governance. The rise of ransomware, exemplified by the WannaCry attack in 2017, marked another turning point, demonstrating how cyberattacks can compromise essential systems worldwide and result in significant financial losses through extortion.[4] In its wake, the emergence of Ransomware-as-a-Service (RaaS) has further escalated the risk, democratizing cybercrime by enabling even low-skilled actors to launch sophisticated attacks.[5] This shift not only has lowered the barrier to entry for malicious actors but also has underscored the urgent need for proactive, enterprise-wide cyber resilience.

Simultaneously, state-sponsored attacks and supply chain breaches, such as the SolarWinds hack in 2020, exposed the vulnerabilities of even the most sophisticated organizations. The pandemic further accelerated digital transformation, expanding the attack surface and making cybersecurity a critical enabler of business continuity.

In response to these evolving threats, cyber defence also evolved dramatically over the past decade, shifting from reactive tools to proactive, integrated platforms. Early years saw the rise of cloud security and next-gen firewalls[6]. By 2020, Zero Trust architecture, DevSecOps[7], and Extended Detection and Response (XDR)[8] became mainstream, embedding security into identity, development, and infrastructure. The later years introduced Secure Access Service Edge (SASE[9]) and Cloud-Native Application Protection Platforms (CNAPP)[10], offering unified, cloud-first defence. The integration of AI and machine learning into threat detection systems allowed for real-time anomaly detection and predictive analytics. Today, post-quantum cryptography is preparing systems for future resilience. Altogether, the decade marked a shift toward automation, integration, and anticipatory defence.

In conclusion, over the past two decades, cybersecurity has evolved from a niche technical function into a cornerstone of modern enterprise strategy. The convergence of escalating threats with rapid digital transformation has redefined its role. Today, cybersecurity is not just about defence; it's about resilience, trust, and competitive advantage.

Cybersecurity timeline: 2015 - 2025

With a comprehensive overview of how the cybersecurity landscape has evolved, we now turn to a year-by-year breakdown, spanning from the launch of the L&G Cyber Security UCITS ETF in 2015 to the present. This structured review offers a clear historical narrative, tracing the key trends, events, and inflection points that have shaped the industry over the ETF's 10 years of existence, and culminating in the milestone we celebrate

[2] https://www.strongdm.com/what-is/yahoo-data-breach
[3] https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
[4] https://www.ibm.com/think/x-force/wannacry-worm-ransomware-changed-cybersecurity
[5] https://www.ibm.com/think/insights/the-rise-of-raas
[6] A Next-Generation Firewall (NGFW) is a network security device that goes beyond traditional firewalls by integrating deep traffic inspection, application-level control, and real-time threat intelligence. While traditional firewalls filter traffic based on IP addresses, ports, and protocols, NGFWs inspect traffic at a much deeper level, understanding what the traffic is, who is sending it, and what it's trying to do. https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-next-generation-firewall.html#tabs-35d568e0ff-item-4bd7dc8124-tab
[7] DevSecOps integrates security into every phase of the software development lifecycle, from design to deployment, rather than treating it as a final step. DevSecOps became critical as agile development and cloud-native architectures demanded faster, safer software releases. https://www.microsoft.com/en-us/security/business/security-101/what-is-devsecops
[8] XDR is an evolution of traditional security tools like EDR (Endpoint Detection and Response). It unifies threat detection, investigation, and response across multiple domains, endpoints, networks, cloud, identity, and applications. https://www.paloaltonetworks.com/cyberpedia/what-is-extended-detection-response-XDR
[9] SASE merges networking and security services into a unified, globally distributed platform that protects users, devices, and applications, regardless of location.
[10] CNAPP is a unified cybersecurity solution designed to secure cloud-native applications throughout their entire lifecycle, from development to deployment and runtime.

today. While not exhaustive, the examples included highlight some of the most significant developments that have defined each year.

2015: The rise of ransomware and insider threats

- Ransomware emerged as a dominant threat. Cryptowall[11] alone earned cybercriminals over $18 million between 2014–2015.[12]
- Insider threats accounted for over half of attacks, highlighting internal vulnerabilities.[11]
- Healthcare became a prime target. Major breaches at Anthem, Premera, and others led to nearly 100 million records being compromised.[13]
- Cybersecurity moved into the boardroom, with CISOs (Chief Information Security Officers) reporting increased support and budgets.[14]
- Top index contributor in 2015: Ahnlab, with a total return of 94.66% and a contribution of 2.11% to the overall index performance.[15]

2016: Cyber threats became national priorities

- The Dyn DDoS attack disrupted major websites (Twitter, Netflix), powered by IoT botnets. It exposed the vulnerability of IoT devices and the fragility of internet infrastructure.[16]
- State-sponsored attacks (e.g., DNC hack) raised geopolitical concerns.[17]
- Governments began treating cyber defence as a national security priority. The Obama administration's Cybersecurity National Action Plan proposed $14 billion in FY2016 and a 35% increase in FY2017, totalling $19 billion in cybersecurity funding.[18]
- The Yahoo breach affected over 1 billion users, emphasizing data security failures and making it one of the biggest single-company data breaches ever recorded.[19]
- In 2016, two-factor authentication became widely available.[20]
- Best index member in 2016: Science Applications International Corporation, with a total return of 89.48% and a contribution of 2.82% to the overall index performance (in USD).

2017: Ransomware evolves into Ransomware-as-a-Service (RaaS)

- WannaCry ransomware attacks caused global disruption.[21]

[11] CryptoWall: a type of ransomware that encrypts your files and demands a ransom, usually in Bitcoin, to unlock them. It spreads through phishing emails, malicious ads, or infected websites. Once it infects a system, it locks access to important files and displays a ransom note. The FBI warned that CryptoWall caused over $18 million in losses in just over a year, including ransom payments, downtime, and recovery costs.
https://www.fbi.gov/contact-us/field-offices/sandiego/news/press-releases/fbi-warns-public-of-cryptowall-ransomware-schemes
[12] https://www.infosecurity-magazine.com/news/ransomware-insider-threats-2015/
[13] https://www.digitalguardian.com/blog/top-4-cybersecurity-trends-2015
https://www.hipaajournal.com/2015-the-year-of-the-healthcare-data-breach-8239/
[14] https://www.smu.edu/news/archives/2015/smu-deason-cybersecurity-risk-study-27oct2015
[15] In USD. From September 28, 2015 until December 31, 2025
[16] In October 2016, hackers unleashed a massive DDoS attack using the Mirai botnet, hijacking thousands of insecure IoT devices like webcams to launch a cyberattack on the Dyn, a Domain Name System Provider, temporarily breaking access to major websites like Twitter, Netflix, and Reddit. It exposed the vulnerability of IoT devices and the fragility of internet infrastructure.
https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
[17] CNN reported that U.S. intelligence agencies concluded the Russian government was behind the Democratic National Committee (DNC) hack in 2016. The goal was to interfere with the U.S. presidential election, influence public opinion, and undermine trust in democratic institutions
https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts
[18] https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan
[19] The breach raised serious concerns about data security and had major implications for Yahoo's reputation and its pending acquisition by Verizon.
https://www.yahoo.com/news/yahoo-says-hackers-stole-information-221214183.html
[20] https://www.paloaltonetworks.com/cyberpedia/what-is-the-evolution-of-multi-factor-authentication
[21] https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

- Ransomware evolved into RaaS, enabling non-technical actors to launch attacks.[22]
- Organizations moved away from centralized IT, accelerating cloud adoption and creating more complex, less controlled data environments. This shift forced a rethink of security strategies. Encryption surged, with widespread adoption of HTTPS[23] and SSL/TLS[24] to protect data in transit.[25]
- Top index contributor in 2017: Sophos Group, with a total return of 140.01% and a contribution of 3.68% to the overall index performance (in USD).

2018: Regulation and collaboration

- Cryptomining surged past ransomware: over 42% of organizations were affected globally, with attackers targeting servers, mobile devices, industrial systems, and cloud infrastructure.[26]
- Cloud infrastructure became a prime target: in 2018, 51% of organizations worldwide experienced cloud-based attacks, including FedEx, Intel, and Honda.[15]
- GDPR came into effect. Under GDPR, organizations must inform authorities within 72 hours of learning that they may have been breached.[27]
- Threat intelligence sharing became strategic: cybersecurity vendors increasingly collaborated to share real-time threat intelligence. Firms recognized that sharing detection data could prevent attacks elsewhere, marking a shift toward coopetition and collective defence.[28]
- Top index contributor in 2018: CyberArk, with a total return of 79.13% and a contribution of 2.35% to the overall index performance (in USD).

2019: From BEC and ransomware to cloud security advancements

- Business Email Compromise (BEC) attacks became more sophisticated, leveraging social engineering and impersonation tactics to defraud organizations.[29]
- Ransomware attacks surged, with threat actors increasingly targeting municipalities, healthcare, and education sectors. Criminal groups diversified operations to include ransomware as a primary revenue stream.[18]
- In 2019, cybersecurity efforts focused on strengthening protection across networks, endpoints, gateways, and devices.[30]
- Cloud Security: at the RSA Conference 2019, Microsoft announced several new capabilities for Azure Security Center, aimed at improving protection for cloud workloads by using machine learning to look at internet traffic and suggest better security settings for virtual machines.[31]
- Top index contributor in 2019: Rapid7, with a total return of 79.78% and a contribution of 2.56% to the overall index performance (in USD).

2020: Pandemic-driven vulnerabilities, remote working and Zero Trust

[22] https://www.sentinelone.com/blog/anti-ransomware-day-2025-10-years-of-raas/
[23] It's the secure version of HTTP, the protocol used to load web pages. The "S" means it uses encryption to protect the data exchanged between your browser and the website.
[24] SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are encryption protocols used to secure data in transit.
[25] https://www.csoonline.com/article/563947/2017-threat-trends-the-year-in-review.html
[26] https://research.checkpoint.com/wp-content/uploads/2018/07/Cyber-Attack-Trends-2018-Mid-Year-Report.pdf
[27] https://gdpr-info.eu/art-33-gdpr/
[28] https://academic.oup.com/cybersecurity/article/4/1/tyy008/5245383
[29] https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
[30] https://www.crn.com/slide-shows/security/the-10-hottest-new-cybersecurity-tools-of-2019
[31] https://azure.microsoft.com/en-us/blog/announcing-new-azure-security-center-capabilities-at-rsa-2019/

- Remote work expanded the attack surface; VPN and RDP exploits surged. According to Kaspersky, brute-force[32] attempts targeting Remote Desktop Protocol (RDP) surged by 242% in 2020.[33]
- COVID-themed phishing campaigns surged, exploiting fear and uncertainty. Cybercriminals groups exploited the COVID-19 pandemic to launch widespread cyberattacks.[34]
- Supply chain attacks: the SolarWinds breach was one of the most significant incidents, compromising multiple U.S. government agencies and corporations.[35]
- Google Cloud introduces BeyondCorp Enterprise, a commercial offering for organizations to adopt Zero Trust security.[36]
- Top index contributor in 2020: Fastly, with a total return of 276.76% and a contribution of 7.36% to the overall index performance (in USD).

2021: Cybersecurity's new normal: supply chain attacks

- In 2021, supply chain attacks have become part of the "new normal". Colonial Pipeline was hit by a ransomware attack, which disrupted fuel supply across the U.S. East Coast.[37]
- Zero Trust architectures gained momentum as VPNs proved inadequate.[38]
- Top index contributor in 2021: Fortinet, with a total return of 141.97% and a contribution of 2.72% to the overall index performance (in USD).

2022: The Ukraine conflict and MFA fatigue redefined cybersecurity priorities

- The Ukraine conflict triggered global cyber warfare and hacktivism. During the early stages of the Ukraine conflict in February 2022, a destructive malware known as HermeticWiper was deployed against Ukrainian infrastructure. Unlike ransomware, HermeticWiper did not seek financial gain, but its sole purpose was to erase data and disable systems, particularly targeting government and critical sectors.[39]
- Threat actors increasingly exploited MFA fatigue as a means of bypassing multi-factor authentication.[40,41]
- Top index contributor in 2022: Ping Identity, with a total return of 24.56% and a contribution of 1.10% to the overall index performance (in USD).

2023: Operation Cookie Monster and the rise of AI-enhanced cybercrime

- Cybercrime and cyber insecurity were ranked as the 8th most severe global risk by the World Economic Forum.[42]

[32] A brute-force attack is a method where attackers use automated tools to try many combinations of usernames and passwords until they find the correct one. When companies rapidly transitioned to remote work, they often didn't have time to properly secure their systems.
[33] https://usa.kaspersky.com/about/press-releases/kaspersky-report-criminals-targeted-remote-work-in-2020
[34] https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-099a
[35] https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack
[36] https://www.onixnet.com/wp-content/uploads/2023/02/Whitepaper-Transforming-Remote-Access-with-Google-Beyond-Corp-Enterprise.pdf
[37] https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
[38] https://www.staysafeonline.org/articles/5-cybersecurity-trends-in-2021
[39] https://www.cyberark.com/resources/blog/hermeticwiper-what-we-know-about-new-malware-targeting-ukrainian-infrastructure-thus-far
[40] After acquiring user credentials often through phishing, attackers would initiate a flood of authentication requests, relying on user error or frustration to gain access.
[41] https://www.cyberdefensemagazine.com/new-threat-report-shows-attackers-increasingly-exploiting-mfa-fatigue/
[42] https://www.weforum.org/publications/global-risks-report-2023/

- In August 2023, the internet was hit by the largest-ever DDoS attack, exploiting a flaw in the HTTP/2 protocol. It peaked at 398 million requests per second, but was successfully mitigated by Google, AWS, and Cloudflare.[43]
- Generative AI transformed both attack and defence strategies. Attackers started to leverage AI for deepfakes, automated phishing, and AI-powered malware.[44]
- Genesis Market, one of the world's largest illicit online marketplaces for stolen digital identities, was dismantled in a major international law enforcement operation called "Operation Cookie Monster." The operation was led by the FBI and Dutch National Police.[45]
- Top index contributor in 2023: CrowdStrike, with a total return of 142.49% and a contribution of 5.07% to the overall index performance (in USD).

2024: The rise of AI defenders

- A faulty update to CrowdStrike's Falcon Sensor caused over 8.5 million Windows systems to crash globally, disrupting critical services across industries. Though not a cyberattack, the incident exposed the fragility of software supply chains and emphasized the need for rigorous update testing and rollback mechanisms.[46]
- A 17-year-old hacker breached Transport for London (TfL) systems, compromising customer data and disrupting services. The attack caused £30 million in damages, highlighting how even low-resource actors can inflict serious harm on public infrastructure.[44]
- AI-Powered defence: cybersecurity providers are actively integrating AI and generative AI into their products.[47]
- SEC mandated breach disclosures within four days.[48]
- EU tightened cyber rules with the Cyber Resilience Act (CRA), designed to strengthen cybersecurity across the entire lifecycle of hardware and software products with digital elements.[49]
- Top index contributor in 2024: Broadcom, with a total return of 110.43% and a contribution of 4.81% to the overall index performance (in USD).

2025: Securing the future: AI, Machine Identity, and Quantum-Safe trust

- Machine Identity management becomes a priority. The rapid rise of autonomous AI agents is creating a major cybersecurity blind spot. With over 45 billion non-human identities expected by year-end, most businesses lack strategies to secure them.[50]
- Post-quantum cryptography: urgent transition to quantum-safe encryption.
- AI enhancing Zero Trust by continuous authentication and authorization based on real-time analysis of user behaviour, device posture, and network conditions.[51]
- Top index contributor in 2025: Cloudflare, with a total return of 100.91% and a contribution of 4.78% to the overall index performance (in USD).[52]

[43] https://www.weforum.org/stories/2023/10/internet-cyber-attack-record/
[44] https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Commercial-Cyber-Security-Trends-2023.pdf
[45] https://www.weforum.org/stories/2023/12/stories-to-read-cybersecurity-2023/
[46] https://www.cm-alliance.com/cybersecurity-blog/top-10-biggest-cyber-attacks-of-2024-25-other-attacks-to-know-about
[47] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer
[48] https://www.sec.gov/files/rules/concept/2025/33-11391.pdf
[49] https://webgate.ec.europa.eu/circabc-ewpp/d/d/workspace/SpacesStore/11f8f4b3-2cca-4b8b-85fe-4e28e5003d7c/download
[50] https://www.weforum.org/stories/2025/09/unsecured-ai-agents-cyberthreat/
[51] https://www.forbes.com/councils/forbestechcouncil/2025/04/16/the-future-of-ai-in-zero-trust-architecture-and-data-regulations/
[52] As of September 28, 2025

Part 2 - from risk to resilience: unlocking cybersecurity's strategic potential

If the first half of the cybersecurity story is about risk, the second is about potential.

While the first part of this article has traced the evolution of cyberspace through the lens of risk, highlighting the blind spots, vulnerabilities, and the relentless pace of adaptation, it is important to recognize that this same dynamic environment also presents significant opportunities.

Cybersecurity is no longer just a defensive concern; it is emerging as a strategic asset. In the next section, we shift focus to explore the structural drivers fuelling the sector's expansion and its growing influence in capital markets, particularly through elevated M&A premiums and robust valuations for cybersecurity companies.

Cybersecurity market outlook: strong growth ahead

The global cybersecurity market is set for robust growth, driven by its vital role in protecting digital infrastructure and enabling secure digital transformation. While estimates vary - Statista projects the market will reach US$197 billion by 2025[53], and Grand View Research places it slightly higher at US$300 billion[54] - all sources highlight the sector's rapid expansion and strategic importance.

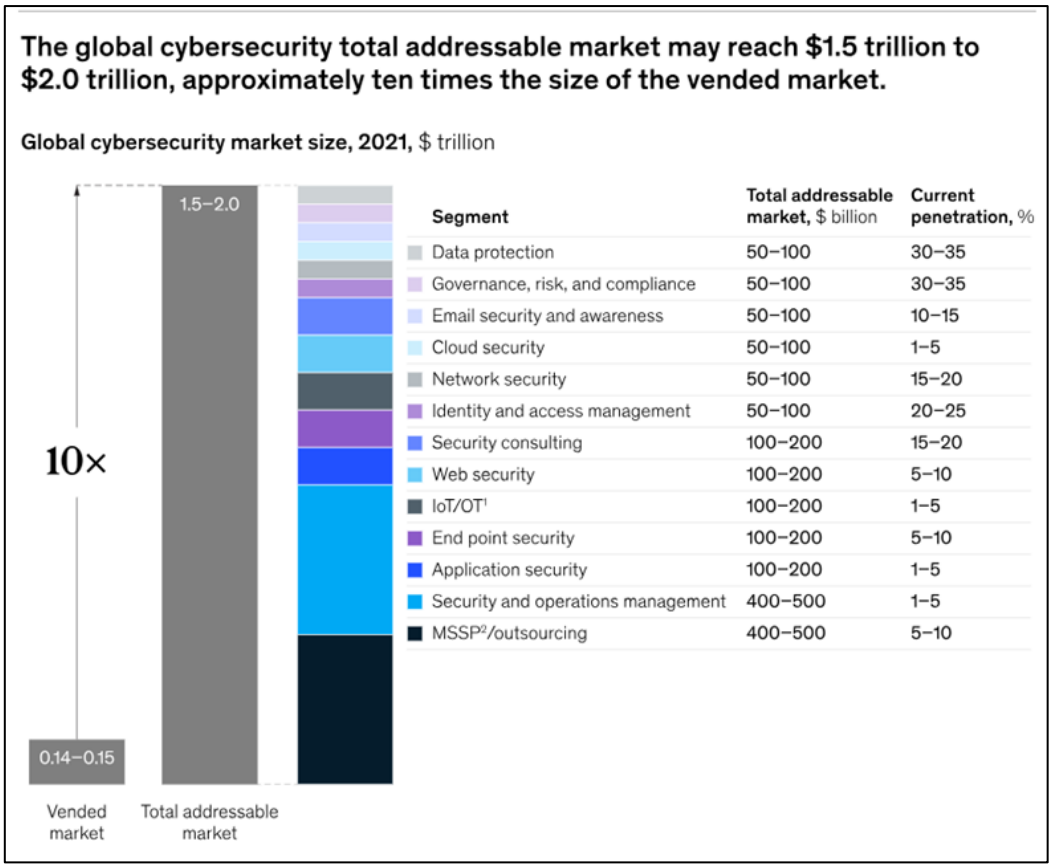
Sustained momentum is expected to continue, with projections varying across sources: Statista forecasts a market size of US$262 billion by 2030, while Grand View Research anticipates it could reach as high as US$500 billion. Despite the differences, the overarching narrative remains clear: cybersecurity is becoming increasingly central to global digital resilience, attracting substantial investment and innovation across industries.

Source: Grand View Research (2025). Assumptions, opinions, and estimates are provided for illustrative purposes only. There is no guarantee that any forecasts made will come to pass.

[53] https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[54] https://www.grandviewresearch.com/industry-analysis/cyber-security-market

What's even more striking is the total addressable market (TAM) for cybersecurity. According to McKinsey, the TAM is estimated to be between US$1.5 trillion and US$2 trillion.[55] This figure reflects the vast unmet demand across industries, driven by the underpenetration of current solutions and the accelerating pace of digital transformation.

With only around 10% market penetration today, the gap between existing spending and full potential highlights a significant opportunity for providers to innovate, scale, and better serve evolving customer needs.



Source: McKinsey & Company (2022). Assumptions, opinions, and estimates are provided for illustrative purposes only. There is no guarantee that any forecasts made will come to pass.

Cybersecurity's new era: from technical concern to strategic priority

The explosive growth of the cybersecurity market is being driven by an urgent and widespread need for protection against increasingly complex digital threats.

According to Statista, the global cost of cybercrime is projected to soar to $13.82 trillion annually by 2028, fuelled by sophisticated attacks such as ransomware, deepfake scams, and AI-powered intrusions. This rapidly evolving threat landscape is compelling governments, enterprises, and critical infrastructure providers to significantly ramp up cybersecurity investments, transforming the sector into one of the most strategically vital and fastest-growing areas of technology.

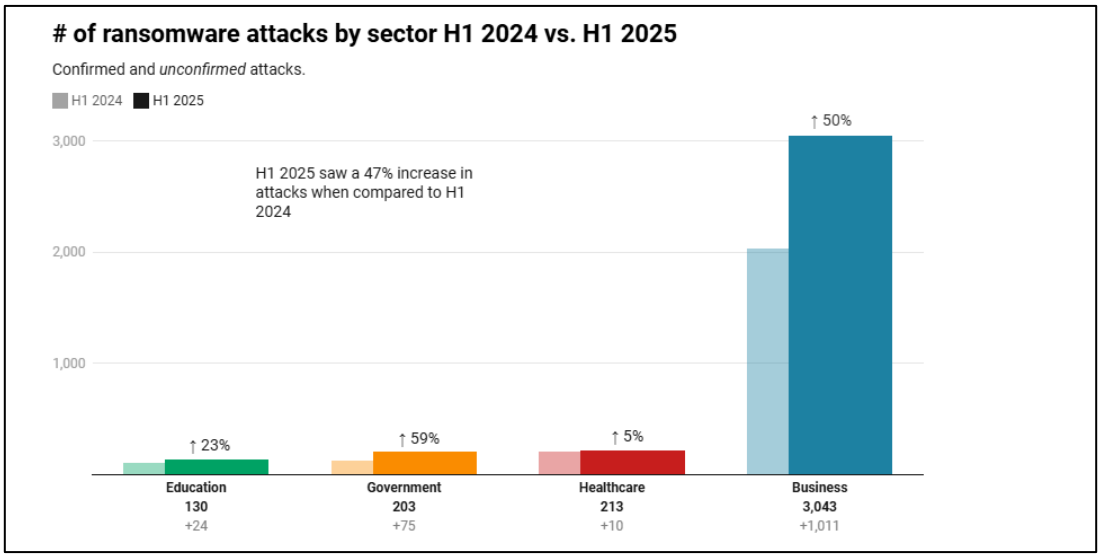
This urgency is echoed by the World Economic Forum, which emphasizes that cybersecurity has become a strategic priority for both governments and enterprises, driven by geopolitical tensions, digital transformation,

[55] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

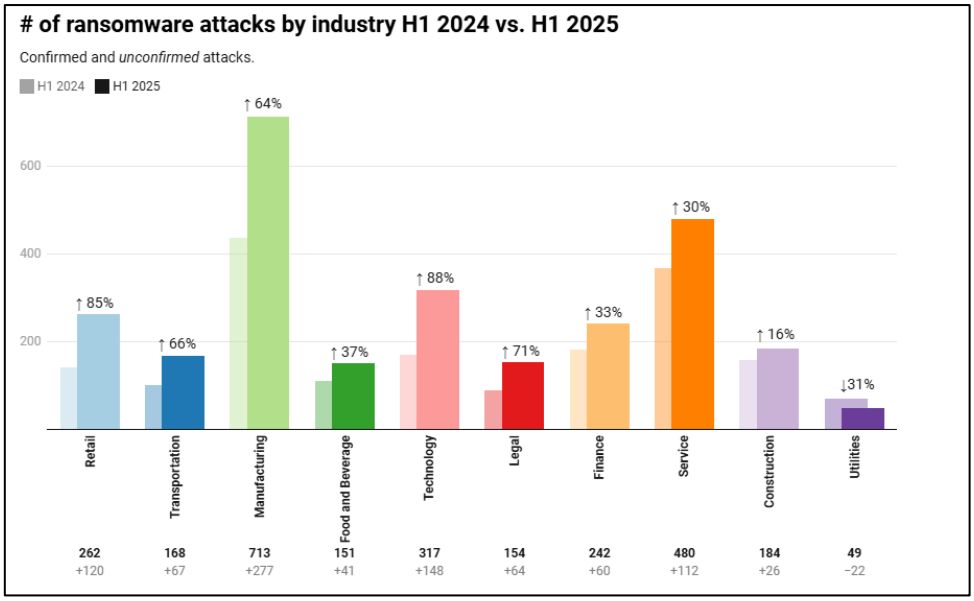
and the increasing sophistication of cyber threats. The Forum's Global Cybersecurity Outlook highlights that nearly 60% of organizations report their cybersecurity strategies are directly influenced by geopolitical instability, and 72% of cyber leaders say risks are rising. These insights reinforce the global consensus: cybersecurity is no longer just a technical concern, but it's a core pillar of national resilience and business continuity.

On the threat side, ransomware remains the top cyber risk concern among executives, with nearly half of respondents identifying it as their primary threat. The report also notes that ransomware tactics are evolving rapidly, making it increasingly difficult for organizations to defend against and recover from such attacks. [56]

This concern is well-founded: in the first half of 2025, ransomware attacks surged with 3,627 incidents logged globally. This represents a 47% increase compared to H1 2024. Government and education sectors saw sharp rises in attacks, up 60% and 23% respectively, while businesses experienced a 50% increase, especially in industries like technology (+88%), retail (+85%), and legal (+71%). Over 17 million records were compromised in confirmed attacks, and the average ransom demand exceeded $1.6 million. Notably, government entities faced the highest ransom demands, with some reaching $12 million, while businesses and healthcare organizations saw lower averages. [57]



[56] https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
[57] https://www.comparitech.com/news/ransomware-roundup-h1-2025/



Source: Comparitech (2025)

Beyond threats: innovation-driven growth in cybersecurity through AI, Cloud Security, and Zero Trust

In response to the escalating threat landscape, several technological and strategic innovations are fuelling the cybersecurity market's rapid expansion.

Artificial Intelligence is transforming threat detection and response. This technology enables real-time anomaly detection, automatic incident triage, and enhanced predictive capabilities, allowing organizations to anticipate and neutralize threats before they materialize. Gartner predicts that by 2030, preemptive cybersecurity solutions powered by AI will account for 50% of IT security spending (up from 5% in 2024), replacing many traditional detection-and-response models.[58]

A recent survey also found that 90% of organizations view Artificial Intelligence and Machine Learning as critical to their cloud strategies, and 32% plan to invest heavily in AI-driven cybersecurity within the next 12 to 18 months.[59]

Indeed, cloud security has emerged as a standalone investment priority. With 60% of the world's corporate data now stored in the cloud, organizations are increasingly focused on securing hybrid and cloud-native environments. This shift is driven by the rise of remote work, the proliferation of SaaS platforms, and the need for scalable, resilient infrastructure. According to SentinelOne, there is growing demand for visibility and automation, with tools like Cloud Security Posture Management (CSPM) and Security Information and Event Management (SIEM) helping organizations monitor, detect, and remediate threats in real time.[60]

[58] https://www.businesswire.com/news/home/20250919589679/en/Gartner-Says-That-in-the-Age-of-GenAI-Preemptive-Capabilities-Not-Detection-and-Response-Are-the-Future-of-Cybersecurity
[59] https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-trends/#key-cloud-security-trends-in-2025
[60] CSPM helps identify and remediate misconfigurations and compliance risks across cloud infrastructure. It continuously monitors cloud environments to ensure security policies are enforced and vulnerabilities are addressed proactively. SIEM systems aggregate and analyse data from across an organization's IT infrastructure. By correlating events and identifying anomalies, SIEM enables security teams to detect threats early and respond efficiently.

Furthermore, Zero Trust Architecture (ZTA) is becoming the new standard for enterprise security. Based on the principle of "never trust, always verify," ZTA enforces strict identity-based access controls and continuous monitoring across all users, devices, and applications. This strategic shift is reflected in the market's rapid growth. The global Zero Trust security market was valued at $37 billion in 2024 and is projected to reach $92 billion by 2030, growing at a CAGR of 16.6%. This expansion is driven by the increasing adoption of cloud computing, the rise of remote work, and the surge in ransomware and insider threats.[61]

Cybersecurity's market momentum: strategic deals and valuation premiums

This explosive growth, driven by both escalating threats and innovation, is not only reshaping enterprise security strategies but also making cybersecurity one of the most compelling investment opportunities across industries.

Over the past few years, the sector has attracted sustained investor interest, even amid macroeconomic headwinds, geopolitical instability, and shifting valuation expectations. The market is witnessing record levels of M&A activity, as strategic buyers and investors seek to consolidate capabilities across high-demand domains such as cloud security, identity management, and AI-driven threat detection.

In 2024, cybersecurity M&A activity remained robust. During that year, Cisco completed its largest acquisition to date, purchasing Splunk for $28 billion to integrate observability and security analytics; Thoma Bravo made a strategic move by acquiring Darktrace for $5.3 billion; Mastercard expanded its threat intelligence capabilities with the $2.65 billion acquisition of Recorded Future; Gen Digital entered the consumer financial security space by acquiring MoneyLion for $1 billion, and Akamai enhanced its API security portfolio with the $450 million acquisition of Noname Security.

In early 2025 alone, major deals included Google's $32 billion acquisition of Wiz, and Palo Alto Networks' proposed $25 billion acquisition of CyberArk, underscoring the strategic value placed on cybersecurity platforms.

The table below summarizes additional key M&A transactions in the cybersecurity sector, highlighting the strategic importance and investor confidence driving consolidation across the industry. Over the past several years, cybersecurity has consistently attracted premium valuations.

Target	Acquirer	Deal Value	Announcement Date	Premium
Darktrace	Thoma Bravo	$5.3 billion	April 26, 2024	20%
Juniper	HPE	$14 billion	January 9, 2024	32%
Splunk	Cisco	$28 billion	September 21, 2023	31%
KnowBe4	Vista Equity	$4.6 billion	October 12, 2022	44%
Ping Identity	Thoma Bravo	$2.4 billion	August 3, 2022	63%
VMware	Broadcom	$61 billion	May 26, 2022	44%
ManTech International	Carlyle	$4.2 billion	May 16, 2022	17%
SailPoint Technologies	Thoma Bravo	$6.9 billion	April 11, 2022	48%
Tufin	Turn/River	$570 million	April 6, 2022	44%
Mandiant	Google	$5.4 billion	March 8, 2022	57%
Mimecast	Permira	$5.8 billion	December 7, 2021	16%

Source: Nasdaq, Bloomberg

[61] https://www.grandviewresearch.com/industry-analysis/zero-trust-security-market-report

Valuation data further confirms the strength of investor interest in cybersecurity.

According to Finro Consulting's mid-2025 analysis, M&A transactions in the sector are achieving some of the highest revenue multiples across the market, particularly in high-demand niches. Cloud Security stands out as the most highly valued segment, with companies in this space averaging 21.7x revenue multiples[62] and reaching up to 35.5x in strategic acquisitions. Identity and Access Management (IAM) and Data Security also demonstrate consistent valuation strength, averaging 15.0x and 16.9x, respectively, across public markets, private funding rounds, and M&A transactions.[63]

In its Q2 2025 Overview and 2025 Outlook report, Solganick observed that valuation multiples for publicly traded cybersecurity companies ranged from a median of 14.2x EV/2025E revenue for high-growth vendors (those growing more than 20%) to a median of 5.3x EV/2025E revenue for low-growth vendors (those growing less than 10%).[64]

These figures show that cybersecurity continues to demonstrate exceptional resilience and strategic relevance, attracting premium valuations and sustained M&A momentum. As threats evolve and digital infrastructure becomes increasingly complex, investor confidence in the sector remains strong, underscoring cybersecurity's role not just as a defensive necessity, but as a dynamic engine of innovation and long-term value creation.

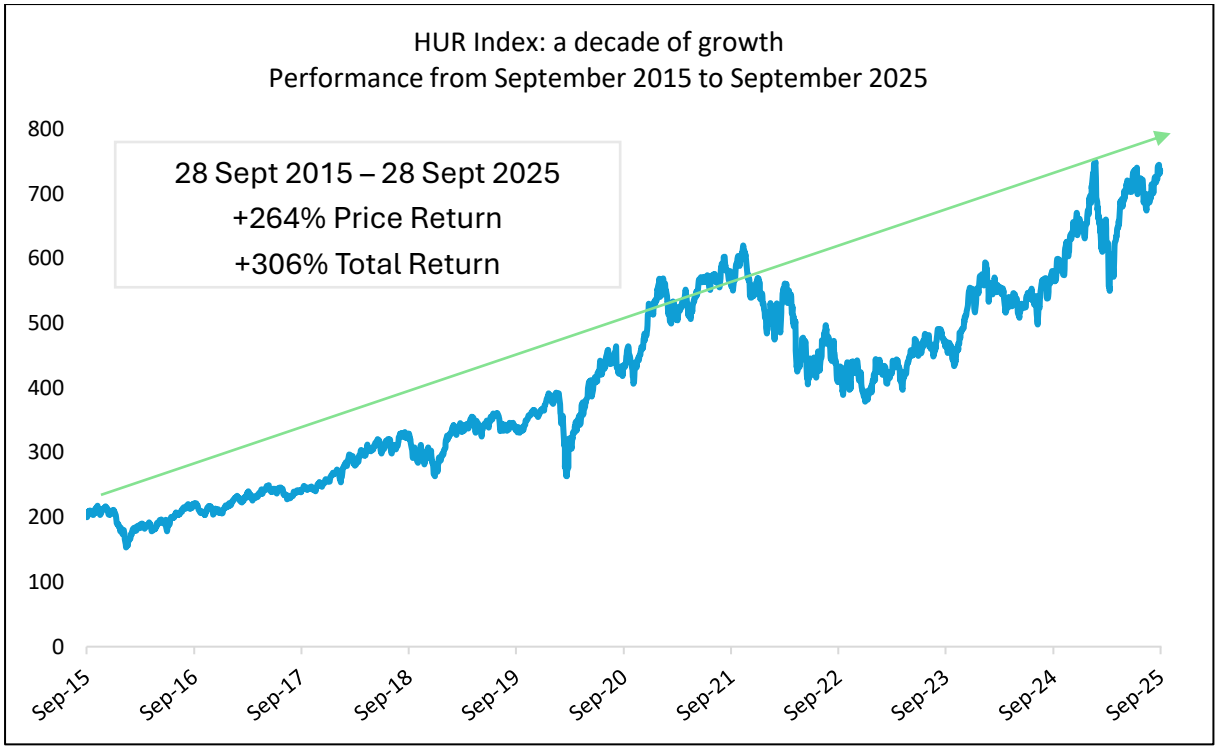
Part 3 - accessing the cybersecurity theme: the ISE Cyber Security UCITS™ Index

Having outlined the strategic importance and long-term opportunity within the cybersecurity space, investors may now be looking for a practical way to gain exposure to the theme. Nasdaq's ISE Cyber Security UCITS™ Index (HUR™) offers a targeted solution, providing access to a diversified set of companies actively involved in providing cyber security technology and services.

Eligibility is determined by the Index Security Selection Committee. To be included, a company must either be a direct service provider in cybersecurity (either as a hardware or software developer) or have a business model built around delivering cybersecurity solutions, where cybersecurity is a key driver of both revenue (minimum 10%) and strategic direction.

Since September 2015, when the L&G Cyber Security UCITS ETF began tracking the index, HUR has delivered a price return of +264% and a total return of +306%, offering investors a clear path to participate in the long-term growth of cybersecurity through a liquid and diversified vehicle.

[62] EV/Revenue
[63] https://www.finrofca.com/news/cybersecurity-valuation-mid-2025
[64] https://solganick.com/wp-content/uploads/2025/07/Solganick-Cybersecurity-MA-Update-Q2-2025.pdf



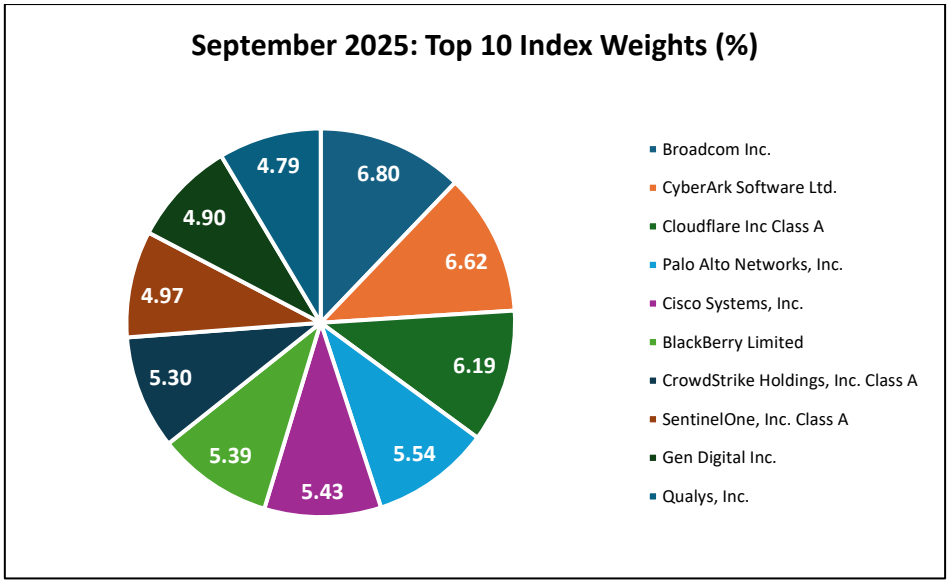
Source: Nasdaq. Data as of 28/9/2025

The HUR Index today - Top 10 constituents

As of September 26, 2025, there were 34 constituents in the index. The top 10 companies represent 56% of the total index weight, while the top 20 companies represent 91% of total index weight.

The top 10 names include notable leaders in the space: Palo Alto Networks (platform-driven cybersecurity leader offering firewalls, cloud security, and AI-powered threat detection), CrowdStrike and SentinelOne (endpoint protection firms using AI and XDR), Cloudflare (leader in edge security and web performance), CyberArk and Qualys (specialists in identity and vulnerability management), Cisco (a global leader in enterprise networking, also offering a broad cybersecurity portfolio including firewalls, endpoint protection, and threat intelligence) and Broadcom (a diversified semiconductor and infrastructure software provider).

These companies represent the most influential players in cybersecurity today, operating across various segments of the Technology and Telecommunications industries, including software, semiconductors, telecommunications equipment, and consumer digital services.



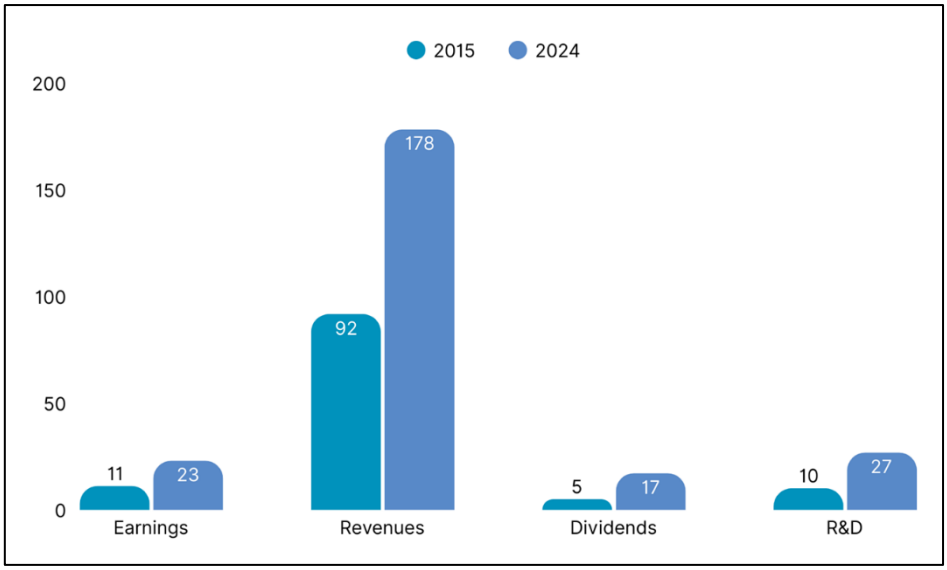
Source: Nasdaq. Data as of 26/9/2025

Among all sub-sectors, software (60% of total index weight) and computer services (20% of total index weight) represent the largest share of the index.

More than just growth: a decade of strong fundamentals

The HUR Index has experienced not only strong performance over the past decade, but performance that has been underpinned by sustained and fundamental growth.

ISE Cyber Security UCITS™ Index ($bn)



Source: Factset

The chart above illustrates the evolution of four key metrics from 2015 to 2024:

- Earnings doubled, rising from $11bn to $23bn.
- Revenues also doubled, increasing from $92bn to $178bn.
- Dividends grew 3.5x, from $5bn to $17bn, reflecting stronger capital returns to shareholders.
- R&D investment surged 2.5x, from $10bn to $27bn, underscoring the sector's sustained commitment to innovation.

Together, these metrics highlight not just headline performance, but the sustained and fundamental growth that has underpinned the HUR Index and its constituents over the past decade, driven by innovation, scale, and increasing shareholder value.

Conclusion - a decade of cyber resilience and opportunity

10 years ago, cybersecurity was a niche concern. On the contrary, today it's a strategic cornerstone of digital resilience and investment. The L&G Cyber Security UCITS ETF has not only tracked this transformation but helped investors participate in one of the most dynamic sectors of the modern economy.

The ISE Cyber Security UCITS™ Index (HUR™) has delivered a +264% total return since the ETF launch date in 2015, reflecting the sector's strength and the index's ability to capture its evolution. As threats grow more complex and technologies more advanced, cybersecurity is no longer just about defence, it's about trust, innovation, and long-term value creation.

Looking ahead, the convergence of AI, Zero Trust, and quantum-safe infrastructure signals a new era of anticipatory security. With digital infrastructure becoming ever more critical, cybersecurity will remain a defining theme for investors seeking resilience and opportunity in a rapidly changing world.

Appendix- Disclaimers

Nasdaq Disclaimer

Nasdaq®, ISE Cyber Security UCITS™, and HUR™ are trademarks of Nasdaq, Inc. The information contained above is provided for informational and educational purposes only, and nothing contained herein should be construed as investment advice, either on behalf of a particular security or an overall investment strategy. Neither Nasdaq, Inc. nor any of its affiliates makes any recommendation to buy or sell any security or any representation about the financial condition of any company. Statements regarding Nasdaq-listed companies or Nasdaq proprietary indexes are not guarantees of future performance. Actual results may differ materially from those expressed or implied. Past performance is not indicative of future results. Investors should undertake their own due diligence

and carefully evaluate companies before investing. ADVICE FROM A SECURITIES PROFESSIONAL IS STRONGLY ADVISED.

L&G Disclaimer

Key Risks

The value of an investment and any income taken from it is not guaranteed and can go down as well as up, and the investor may get back less than the original amount invested. Past performance is not a guide to future performance.

- The value of an investment and any income taken from it is not guaranteed and can go down as well as up; you may not get back the amount you originally invested.
- An investment in the ETF involves a significant degree of risk. Any decision to invest should be based on the information contained in the relevant prospectus. Prospective investors should obtain their own independent accounting, tax and legal advice and should consult their own professional advisers to ascertain the suitability of the ETF as an investment.
- The value of the shares in the ETF is directly affected by increases and decreases in the value of the Index. Accordingly the value of a share in the ETF may go up or down and a shareholder may lose some or the entire amount invested.
- The ETF's ability to closely track the Index will be affected by its ability to purchase and/or sell the Index constituents and any legal or regulatory restrictions or disruptions affecting them.
- The ETF's ability to closely track the Index will also be affected by transaction costs and taxes incurred when adjusting its investment portfolio generally and/or to mirror any periodic adjustments to the constituents of the Index. There can be no certainty that ETF shares can always be bought or sold on a stock exchange or that the market price at which the ETF shares may be traded on a stock exchange will reflect the performance of the Index.
- The ETF is subject to the risk that third party service providers (such as a bank entering into swaps with the ETF or the ETF's depositary) may go bankrupt or fail to pay money due to the ETF or return property belonging to the ETF.
- As the Index includes micro, small and medium-sized publicly traded companies, the ETF is subject to the risk that such companies may be more vulnerable to adverse business or economic events and greater and more unpredictable price changes than larger companies or the stock market as a whole.
- The ETF is subject to the risks associated with technology-focused companies that are particularly vulnerable to rapid developments in technology (which may leave their products out-of-date), government regulation and competition from domestic and foreign competitors who may have lower production costs. Such companies may also have difficulties establishing and maintaining patents, copyrights, trademarks and trade secrets relating to their products which could negatively affect their value.
- There is no capital guarantee or protection on the value of the ETF. Investors can lose all the capital invested in the ETF.
- Please refer to the “Risk Factors” section of the Issuer’s Prospectus and the Fund Supplement.
- This Fund may have underlying investments that are valued in currencies that are different from the currency of this share class, in which case exchange rate fluctuations will impact the value of your investment. In addition, the return in the currency of this share class may be different to the return in your own currency.

Important Information

The information in this document is for professional investors and their advisers only. This document is for information purposes only and we are not soliciting any action based on it. The information in this document is not an offer or recommendation to buy or sell securities or pursue a particular investment strategy and it does not constitute investment, legal or tax advice. Any investment decisions taken by you should be based on your

own analysis and judgment (and/or that of your professional advisers) and not in reliance on us or the Information.

This document does not explain all of the risks involved in investing in the fund or investment strategy. No decision to invest in the fund or investment strategy should be made without first reviewing the prospectus, key investor information document and latest report and accounts for the fund, which can be obtained from https://fundcentres.landg.com/.

No party shall have any right of action against L&G in relation to the accuracy or completeness of the information in this document. The information and views expressed in this document are believed to be accurate and complete as at the date of publication, but they should not be relied upon and may be subject to change without notice. We are under no obligation to update or amend the information in this document. Where this document contains third-party data, we cannot guarantee the accuracy, completeness or reliability of such data and we accept no responsibility or liability whatsoever in respect of such data.

This financial promotion is issued by Legal & General Investment Management Limited.

The risks associated with each fund or investment strategy are set out in the key investor information document and prospectus or investment management agreement (as applicable). These documents should be reviewed before making any investment decisions. A copy of the English version of the prospectus and the key investor information document for each fund is available at www.lgim.com and may also be obtained from your Client Relationship Manager. Where required under national rules, the key investor information document will also be available in the local language of the relevant EEA Member State.

A decision may be taken at any time to terminate the arrangements made for the marketing of the fund in any EEA Member State in which it is currently marketed. In such circumstances, shareholders in the affected EEA Member State will be notified of this decision and will be provided with the opportunity to redeem their shareholding in the fund free of any charges or deductions for at least 30 working days from the date of such notification.

Information on sustainability-related aspects on the funds is available on https://fundcentres.landg.com/. The decision to invest in the funds should take into account all the characteristics or objectives of the fund as described in its prospectus and in the key investor information document relating to the fund.

No party shall have any right of action against L&G in relation to the accuracy or completeness of the information in this document. The information and views expressed in this document are believed to be accurate and complete as at the date of publication, but they should not be relied upon and may be subject to change without notice. We are under no obligation to update or amend the information in this document. Where this document contains third-party data, we cannot guarantee the accuracy, completeness or reliability of such data and we accept no responsibility or liability whatsoever in respect of such data.

The information contained in this email is strictly confidential and may be subject to legal privilege or protected by other legal rights. Access, copying or re-use of this email (or any part thereof) by anyone other than the intended recipient is strictly prohibited. If you are not the intended recipient of this email, please notify the sender immediately and delete all copies from your computer. To the extent permitted by law we do not accept any liability for any virus infection, malware or for the transmission of harmful content through this email. We reserve the right to monitor, and retain emails as permitted by applicable law. View our privacy policy.

For investors in Switzerland:

This information provided herein does not constitute an offer of the Funds in Switzerland pursuant to the Swiss Federal Law on Financial Services ("FinSA") and its implementing ordinance. This is solely an advertisement pursuant to FinSA and its implementing ordinance for the Funds.

Swiss Representative and Paying Agent: State Street Bank International GmbH Munich, Zurich Branch Beethovenstraβe 19, 8007 Zurich, Switzerland.

Availability of Documents: The prospectus, Key Information Documents (KIDs), the instruments of incorporation, annual report and subsequent semi-annual report and additional relevant documentation of the above-mentioned collective investment schemes are available free of charge from the Swiss representative and from Legal & General Investment Management Limited, One Coleman Street, London, EC2R 5AA, GB.

In the European Economic Area, this document is issued by LGIM Managers (Europe) Limited, authorised and regulated by the Central Bank of Ireland as a UCITS management company (pursuant to European Communities (Undertakings for Collective Investment in Transferable Securities) Regulations, 2011 (as amended) and as an alternative investment fund manager (pursuant to the European Union (Alternative Investment Fund Managers) Regulations 2013 (as amended). LGIM Managers (Europe) Limited's registered office is at 70 Sir John Rogerson's Quay, Dublin, 2, Ireland and it is registered with the Irish Companies Registration Office under company no. 609677.

LGIM Managers (Europe) Limited operates a branch network in the European Economic Area, which is subject to supervision by the Central Bank of Ireland. In Italy, the branch office of LGIM Managers (Europe) Limited is subject to limited supervision by the Commissione Nazionale per le società e la Borsa ("CONSOB") and is registered with Banca d'Italia (no. 23978.0) with registered office at Piazza della Repubblica 3, 20121 - Milano (Companies' Register no. MI - 2557936). In Sweden, the branch office of LGIM Managers (Europe) Limited is subject to limited supervision by the Swedish Financial Supervisory Authority ("SFSA"). In Germany, the branch office of LGIM Managers (Europe) Limited is subject to limited supervision by the German Federal Financial Supervisory Authority ("BaFin"). In the Netherlands, the branch office of LGIM Managers (Europe) Limited is subject to limited supervision by the Dutch Authority for the Financial Markets ("AFM") and it is included in the register held by the AFM and registered with the trade register of the Chamber of Commerce under number 74481231. Details about the full extent of our relevant authorisations and permissions are available from us upon request.

Details about the full extent of our relevant authorisations and permissions are available from us upon request. For further information on our products (including the product prospectuses), please visit our website.

Legal & General Investment Management Limited, authorised and regulated by the Financial Conduct Authority, No. 119272. Registered in England and Wales No. 02091894 with registered office at One Coleman Street, London, EC2R 5AA.