Why Cybersecurity, Why Now: The Imperative of Our Time

September 2025

Ilaria Sangalli, *Index Research Lead*

In recognition of Cybersecurity Awareness Month, this two-part article series explores the critical importance and rapid evolution of cybersecurity in today's digital landscape.

The first article, "Why Cyber, Why Now: The Imperative of Our Time," addresses the growing urgency surrounding cyber resilience, driven by escalating global threats, technological complexity, and the increasing interdependence of digital systems.

The second, "25 Years of Evolving Battlefields: How Innovation Shapes Cyber Threats and Security," offers a retrospective analysis of how cyber threats and defensive strategies have evolved over the past quarter-century, highlighting key inflection points and innovations that have shaped the modern security ecosystem.

Together, these articles aim to foster greater awareness, strategic insight, and a shared sense of responsibility across all levels of the organization.

Introduction

In the last decade, digital transformation has redefined how we live, work, and interact. Technologies like cloud computing, IoT, AI, and 5G have driven unprecedented innovation, but they have also created new vulnerabilities. As our dependence on digital systems deepens, cybersecurity has evolved from a technical concern into a strategic imperative.

Today's cyber threats are no longer abstract or isolated. From ransomware attacks on hospitals to state-sponsored campaigns targeting critical infrastructure, the risks are tangible, global, and increasingly life-threatening.

Ransomware, in particular, has become the business model of modern cybercrime. Meanwhile, artificial intelligence is reshaping both sides of the cybersecurity equation. On the defensive front, AI enhances threat detection and response. But offensively, AI is accelerating the speed, scale, and sophistication of attacks.

This article explores the forces reshaping the cybersecurity landscape and sets the stage for a broader journey through the evolution of cyber threats, the advancement of cyber-defined strategies, and ultimately, the emergence of cybersecurity as a strategic opportunity.

The digital explosion and expanding attack surface

To understand the urgency of today's cybersecurity challenge, we begin by examining how emerging technologies have expanded the digital attack surface. These innovations, while transformative, have introduced new vulnerabilities that cybercriminals and hostile actors are quick to exploit:

Smartphones: central to daily life, used for everything from banking to dating, yet constantly targeted by phishing scams and invasive apps.[1]

Cloud computing: the backbone of modern business, enabling remote work and global collaboration, but a single misconfiguration can expose millions of records.[2]

AI: enhances threat detection but also enables attackers to automate scams and create convincing deepfakes, that can impersonate CEOs, politicians, or even loved ones, tricking people into transferring money or sharing sensitive data.[3]

IoT Devices: from smart fridges to wearable health monitors, they bring convenience but often lack basic security, making them vulnerable to botnets and DDoS attacks.[4]

5G: increases data speed and volume, expanding the digital attack surface and making real-time threat detection and response significantly more complex.[5]

From pandemic to pipeline: navigating risk in a digitally interconnected world

In recent years, cybersecurity has evolved from a behind-the-scenes technical issue to a core part of business strategies. This shift has been driven by rapid digital adoption, rising geopolitical tensions, and increasingly sophisticated attacks that expose deep vulnerabilities across industries.

The COVID-19 pandemic has accelerated a shift to remote work and digital transformation, dramatically expanding the attack surface across industries. Shadow IT environments, where employees use unauthorized tools, became widespread, with 41% of staff operating in such setups, a figure expected to rise to 75% by 2027.[6]

Meanwhile, escalating geopolitical tensions have fuelled a surge in state-sponsored cyber threats, targeting critical infrastructure. Europol reports that criminal entities are increasingly forming strategic alliances with state-sponsored hybrid threat actors.[7][8] Supporting this trend,

[1] https://www.forbes.com/sites/zakdoffman/2025/02/20/new-iphone-android-warning-your-phone-is-now-at-risk/

[2] https://www.forbes.com/councils/forbestechcouncil/2025/04/08/why-cloud-misconfigurations-remain-a-top-cause-of-data-breaches/

[3] https://www.paloaltonetworks.com/cyberpedia/ai-risks-and-benefits-in-cybersecurity

[4] https://www.checkpoint.com/cyber-hub/network-security/what-is-iot/iot-botnet/

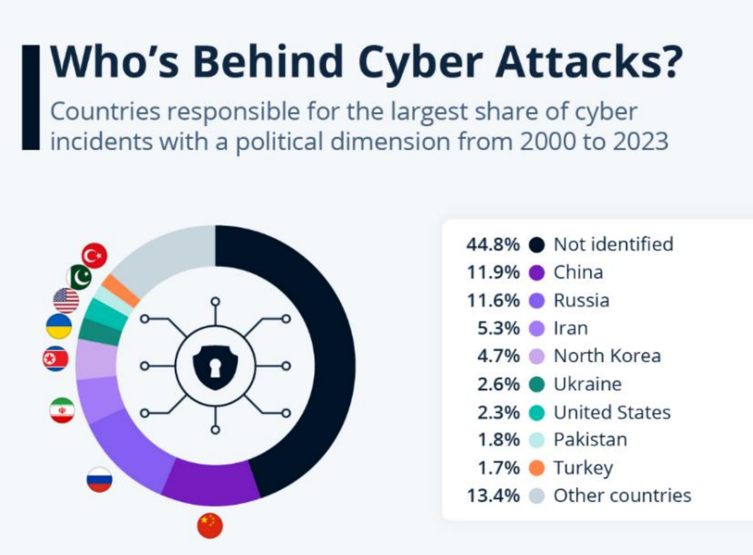
[5] https://digitaldefynd.com/IQ/5g-cyber-security-risks/

[6] https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024

[7] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

[8] Entities (state or non-state) that use a coordinated mix of coercive and subversive activities across multiple domains to exploit vulnerabilities and cause harm below the threshold of open aggression.

data from the European Repository of Cyber Incidents (EuRepoC) indicates that between 2000 and 2023, over 2,500 politically motivated cyberattacks occurred worldwide, involving nearly 700 known groups. Nearly one-third of the politically motivated cyberattacks analysed were attributed to state actors or affiliated groups, with a comparable share linked to politically driven non-state entities. Approximately half of these incidents targeted political figures, parties, or institutions, and 20% aimed at critical infrastructure.[9]



Source: Statista, EuRepoC

Furthermore, in today's interconnected economy, a single breach can also ripple across entire sectors. The SolarWinds attack in 2020 is a stark example: hackers embedded malware into routine software updates, compromising up to 18,000 organizations, including U.S. federal agencies and Fortune 500 companies, through a trusted vendor.[10]

The cost of cybercrime - the rising economic threat of the digital age

In today's digital world, one of the most significant risks posed by cybersecurity threats is financial loss.

As more financial data is stored online to facilitate digital payments, sensitive information such as credit card numbers, bank credentials, and investment accounts become prime targets for cybercriminals. The consequences are costly, not only in terms of money, but also time, effort, and reputational damage as victims work to restore their financial credibility.

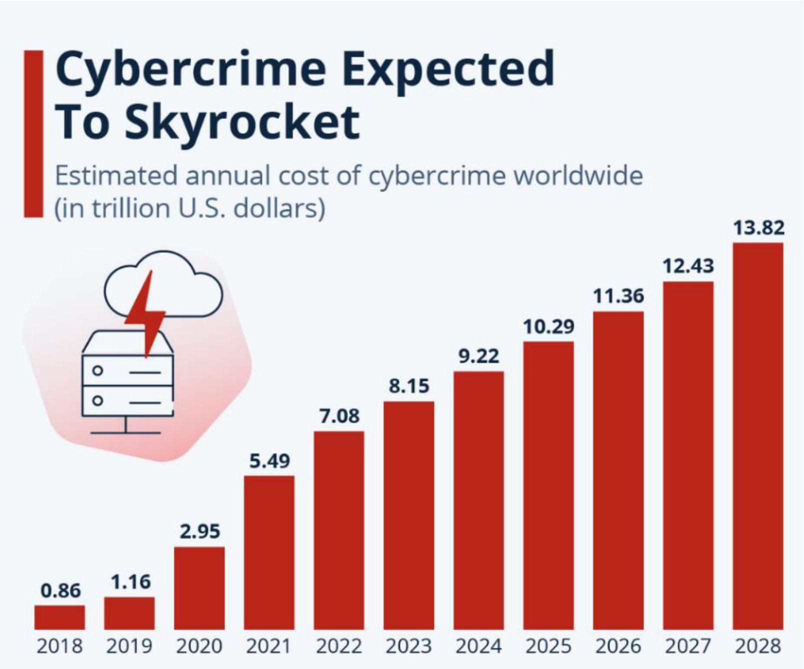
In 2023, global cybercrime was estimated to cost $8 trillion, rising to $9 trillion in 2024, and projected to reach $10 trillion in 2025. By 2028, this figure could approach $14 trillion,[11] reflecting a massive and growing economic burden.

https://defence-industry-space.ec.europa.eu/document/download/3b90af44-dbf6-4ea7-a24a-b6c60305c9be_en?filename=Factsheet%20-%20Countering%20Hybrid%20Threats.pdf

[9] https://www.statista.com/chart/31805/countries-responsible-for-the-largest-share-of-cyber-incidents/

[10] https://www.cfcs.dk/globalassets/cfcs/dokumenter/rapporter/en/CFCS-solarwinds-report-EN.pdf

[11] https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/



Source: Statista

If cybercrime were a national economy, it would rank as the third largest in the world, trailing only the United States and China, based on its estimated economic impact.[12,13]

For comparison, while drug trafficking has long been considered one of the most profitable illicit industries, generating hundreds of billions of dollars annually according to the United Nations Office on Drugs and Crime, cybercrime now surpasses it significantly, with global economic impacts estimated in the trillions of dollars each year.[14]

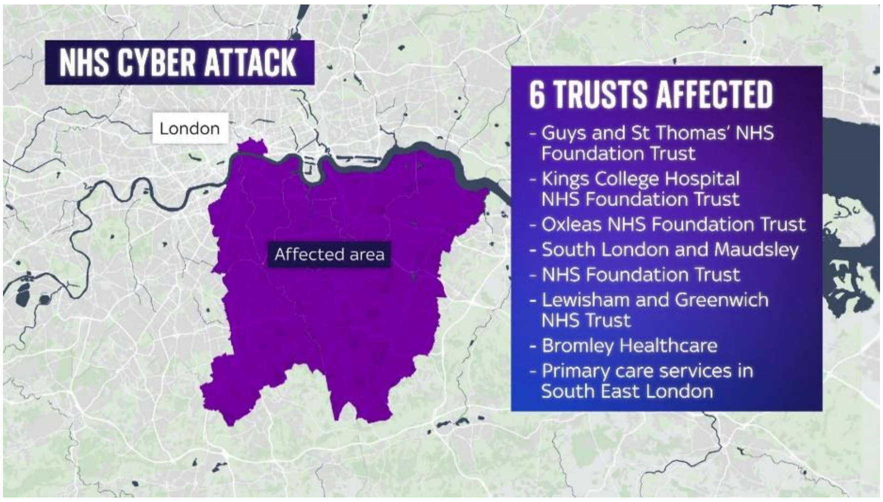
Unlike drug trafficking, which is constrained by physical borders and logistics, cybercrime spreads instantly, invisibly, and globally. Its digital nature allows attackers to reach victims across continents with minimal effort, making it not just a financial threat, but a strategic challenge for governments, businesses, and society.

Not just data breaches – when attacks hit infrastructure and lives

Cyberattacks are not just about stolen data or financial loss, they can disrupt essential services and, in some cases, endanger lives.

An example of this occurred in June 2024, when a ransomware attack on Synnovis, a pathology provider for several NHS hospitals in London, led to widespread disruption of diagnostic services. The attack delayed over 10,000 appointments, postponed 1,710 operations, and disrupted 1,100 cancer treatments. Tragically, one patient died as a result of delayed blood test results, marking the first confirmed fatality linked directly to a cyberattack on the NHS. This incident underscores the life-or-death consequences of cybersecurity failures and highlights the urgent need for robust protections across healthcare systems.[15]

[12] https://www.weforum.org/stories/2023/02/cybersecurity-in-an-era-of-polycrisis/
[13] https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=true
In 2024 USD GDP values: ~29 trillion for the U.S., ~18.7 trillion for China, and ~4.7 trillion for Germany
[14] https://www.unodc.org/documents/data-and-analysis/WDR_2025/WDR25_B1_Key_findings.pdf
[15] https://www.infosecurity-magazine.com/news/patient-death-linked-nhs-cyber/


NHS CYBER ATTACK
London
Affected area
6 TRUSTS AFFECTED
- Guys and St Thomas' NHS Foundation Trust
- Kings College Hospital NHS Foundation Trust
- Oxleas NHS Foundation Trust
- South London and Maudsley
- NHS Foundation Trust
- Lewisham and Greenwich NHS Trust
- Bromley Healthcare
- Primary care services in South East London

Source: SkyNews

Other critical sectors face similar risks. In 2021, the Colonial Pipeline, which supplies nearly half of the fuel to the U.S. East Coast, was hit by a ransomware attack that forced a multi-day shutdown, causing fuel shortages, panic buying, and economic disruption. The company paid a $4.4 million ransom to restore operations.[16]

That same year, a cyberattack on the Oldsmar Water Plant in Florida saw hackers attempt to poison the water supply by increasing levels of sodium hydroxide. Fortunately, the attack was caught in time, but it exposed serious vulnerabilities in public infrastructure.[17]

Protecting data is no longer just about safeguarding information, it's about protecting people, services, and lives.

Ransomware: the business model of modern cybercrime

The previous examples show that cyber threats are no longer confined to digital spaces. They can have real-world, physical impacts on public safety and national resilience.

At the heart of many of these high-impact events lies a common and increasingly dominant threat: ransomware.[18] Its evolution from opportunistic attacks to a global, service-based industry reflects the professionalization of cybercrime itself.

In 2024, ransomware attacks surged to over 5,200 incidents worldwide, marking a 15% increase from the previous year. This growth follows a staggering 77% spike in 2023, underscoring the relentless pace of cybercriminal activity.[19]

The Sophos State of Ransomware 2024 report reveals a dramatic escalation in the financial impact of ransomware attacks. Over the past year, the average ransom payment surged by 500%, climbing from $400,000 in 2023 to $2 million in 2024. But ransom payments are only part of the story, as recovery costs excluding ransom rose to $2.73 million, up nearly $1 million from

https://cybernews.com/cybercrime/patient-death-linked-to-nhs-cyberattack/

[16] https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[17] https://www.cbsnews.com/news/florida-water-hack-oldsmar-treatment-plant/

[18] A type of malware that prevents you from accessing your device or the data stored on it, usually by encrypting your files. Criminals then demand a ransom in exchange for decryption

[19] https://www.dni.gov/files/CTIIC/documents/products/Worldwide_Ransomware_2024.pdf

the previous year. The most common root causes of attacks were exploited vulnerabilities (32%), followed by compromised credentials (29%) and malicious emails (23%).[20]

Looking ahead, Cybersecurity Ventures predicts that ransomware is projected to cost victims $275 billion per year by 2031, with attacks occurring every two seconds.[21]

AI-Powered threats: speed, scale, and autonomy

While ransomware has become the most visible and financially damaging form of cybercrime, it is only one part of a rapidly evolving threat landscape. The next frontier is being shaped by artificial intelligence, a technology that is not only transforming how we defend against attacks, but also how they are launched.

As AI increasingly augments both cyberattacks and defences, the landscape of cybersecurity is shifting from manual to autonomous threats, and from reactive to predictive defence strategies.

On the offensive side, AI-generated spear phishing[22] is now more effective than human-crafted attacks. In 2023, AI lagged behind humans by 31%, but by early 2025, it had overtaken them, with a 24% higher success rate based on user click-through rates.[23] This jump is driven by the rise of agentic AI, autonomous systems capable of learning, adapting, and executing tasks with minimal human input. These agents can now mimic emotional cues, personalize messages, and scale attacks with unprecedented precision.[24]

Meanwhile, malware development is accelerating. AI can now auto-generate malicious code in hours, and generative AI could reduce the time needed to exfiltrate sensitive data to just 25 minutes, compared to hours or days in previous years. These advances mark a turning point: cyberattacks are no longer simply getting faster, they are also becoming smarter, more targeted, and increasingly autonomous.[25]

On the defence side, speed pays off. The IBM 2025 Cost of a Data Breach Report found that organizations leveraging AI and automation detect and contain breaches 80 days faster than those without these technologies, resulting in an average cost reduction of $1.9 million per breach.[26]

Key takeaways

The picture that emerges is clear: cybersecurity has evolved from a niche technical concern into a central challenge of the digital era. From the proliferation of connected devices to the weaponization of AI, the threat landscape is expanding in speed, scale, and complexity.

The consequences are not only financial, but societal, geopolitical, and deeply human. Yet within this escalating risk lies a powerful truth: the same forces that make us vulnerable also present

[20] https://www.sophos.com/en-us/press/press-releases/2024/04/ransomware-payments-increase-500-last-year-finds-sophos-state

[21] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

[22] AI-generated spear phishing is when cybercriminals use artificial intelligence to create highly convincing fake messages that are designed to trick specific people. These messages often look like they come from someone you know or trust, and they're personalized using information about you, making them much harder to spot as fake.

[23] In 2023, AI-generated phishing emails were 31% less effective than those written by humans. By early 2025, AI had overtaken humans, achieving a 24% higher success rate, measured by click-through rates (i.e., how often recipients clicked on malicious link)

[24] https://www.securityweek.com/ai-now-outsmarts-humans-in-spear-phishing-analysis-shows/

[25] https://www.securityweek.com/cyber-insights-2025-malware-directions/

[26] https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91

an opportunity. Cybersecurity, when approached strategically, can become a driver of trust, innovation, and resilience.

This is why investors are increasingly drawn to the sector. Global spending on cybersecurity is expected to reach $200 billion in 2025, driven by high-profile breaches and the growing complexity of digital ecosystems.[27] Cybersecurity companies benefit from structural growth and recurring revenues. Additionally, the integration of AI and automation is opening new frontiers, allowing companies in the space to expand their capabilities and capture market share through innovation and consolidation.

Disclaimer:

Nasdaq® is a 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.

[27] Source: Statista