Cybersecurity: From National Security to the Corporate Balance Sheet

Published October 15, 2025

Christopher Gannatti, CFA
Global Head of Research

Key Takeaways

- The Heathrow cyber disruption in September 2025 highlights how third-party vulnerabilities can ripple across national security, corporate stability and investor portfolios.
- Diverging regulatory approaches, Europe's strict mandates versus the U.S.'s reactive stance, are shaping uneven but accelerating global demand for cybersecurity solutions.
- With spending forecast to more than double by 2026, the WisdomTree Cybersecurity Fund (WCBR) seeks to offer exposure to the firms building the digital infrastructure underpinning growth and innovation.

October marks **Cybersecurity Awareness Month**, a timely backdrop for examining how digital defense now spans national security, corporate resilience and investor opportunity. The Heathrow disruption and rising supply chain attacks remind us: these layers aren't separate stories, but one connected reality.

When people talk about cybersecurity, the conversation often fractures. One camp gravitates toward the macro story: hostile states, ransomware gangs, hospitals or pipelines going dark. The other focuses on the micro: endpoint software, firewalls, identity tools. Rarely are these perspectives stitched into one narrative. Yet they belong together. Cybersecurity is simultaneously a matter of national strategy, corporate resilience and investor opportunity. And, in 2025, all three are colliding.

Even as cyberthreats mount globally, recent events at Heathrow illustrate how fragile critical infrastructure remains—even in tightly regulated and security-conscious locales. In September 2025, a **cyber-related disruption** that struck check-in and boarding systems at Heathrow (alongside airports in Berlin and Brussels) was traced back to a service provider, Collins Aerospace.[1] Although no definitive attribution had been confirmed at the time, experts warned that the event underscores how vulnerabilities in third-party systems can ripple outward, creating national security, economic and reputational risks.

Cybercrime as National Security

It has become routine to call cyberspace the "fifth domain" of warfare. But behind the cliché lies a blunt reality: the distinction between crime and war is collapsing. In 2024, financially motivated attackers accounted for almost four times as many intrusions as state-backed groups.[2] Yet whether a hospital is

crippled by ransomware or a state actor's wiper malware, the effect is the same—patients wait, care is delayed, and lives are put at risk.

One study found in-hospital mortality spikes by 35%–41% during ransomware disruptions.[3] These are not nuisance events. They are national security crises in disguise, bleeding out through the balance sheets of hospitals, logistics companies and critical infrastructure.

And the scale is staggering. A single ransomware attack forced 150 U.S. plasma donation centers offline. Another wave knocked 25 Romanian hospitals out of service. In the U.S., the FBI estimates that business email compromise alone has drained **$55 billion** from global firms since 2013.[4] When such figures are stacked against the gross domestic product (GDP) of smaller nations, the point is clear: cybercrime is an economy-level risk.

The Criminal-State Nexus

Cybercrime is no longer a cottage industry. It is an ecosystem, with suppliers of stolen credentials, malware developers and "initial access brokers."[5] In that marketplace, states shop alongside criminals.

Russia has drawn deeply on this ecosystem in its campaigns against Ukraine and NATO[6] countries. GRU[7]-linked APT44[8] has redeployed ransomware variants purchased from criminal forums. North Korea flips the model: its hackers generate revenue directly for the regime, stealing **$3 billion in cryptocurrency between 2017 and 2023**. Iran and China blur the lines further, embedding ransomware or extortion inside espionage campaigns, partly to confuse attribution.[9]

This is the murky zone that policy makers and companies must now navigate. The same malware kit can power a petty heist one week and an assault on critical infrastructure the next. The neat division between crime and geopolitics no longer holds.

Policy Playing Catch-Up

Governments have been forced to respond, though the pace and style vary across geographies.

- **Europe** has gone the furthest. The *NIS2 Directive*, effective in 2023, expands obligations across sectors: telecoms, social media, cloud services and even public administrations. It harmonizes enforcement, imposes strict reporting timelines and explicitly addresses supply chain risks.[10]
- **The UK** raised the stakes in 2025 with its *Cyber Security and Resilience Bill*. Regulators can now designate "critical suppliers," pull smaller firms into scope if they are pivotal and require incident notifications within 24 hours. In emergencies, the government can even direct companies to act.[11]
- **The U.S.**, by contrast, has been more piecemeal. CISA[12] sets baselines, and both administrations have invested in supply chain resilience. But compared with Europe's centralized, punitive approach, the U.S. patchwork looks softer.

For businesses, these differences matter. In Europe, compliance is non-negotiable and costly. In the U.S., adoption follows breaches rather than mandates. For investors, that means uneven demand curves: a steady regulatory bid in Europe, more volatile spending cycles in America.

Cybersecurity as Growth Infrastructure

Too often, cybersecurity is framed as a drag—a necessary but unproductive cost. That framing is increasingly obsolete. Cybersecurity is growth infrastructure.

The UK government was explicit: *"There is no growth without stability."*[13] That isn't political rhetoric; it's basic economics. A ransomware attack that halted customs in Costa Rica paralyzed trade, causing losses measured in millions of dollars per day.[14] Attacks on cloud providers cascade into lost productivity across industries.

Secure digital infrastructure is to the 21st century what ports and highways were to the 20th. It underpins innovation, attracts investment and makes possible the layering of new technologies. Without resilient networks, AI adoption, internet of things (IoT) expansion and cloud migration stall. The fastest way to derail innovation is to ignore defense.

Where Companies Fit

The corporate layer translates policy and threat into solutions. A snapshot of leading firms illustrates the ecosystem:

- **Edge defenders**: Examples include Cloudflare, Akamai, Fastly—guarding the internet's outer perimeter against distributed denial of service (DDoS) attacks and traffic manipulation.
- **Network security leaders**: Examples include Zscaler, Palo Alto, Fortinet, Check Point—designing cloud firewalls and zero-trust architectures.
- **Endpoint sentinels**: Examples include CrowdStrike, SentinelOne, Trend Micro—monitoring devices and servers for intrusions.
- **Observability and resilience**: Examples include Datadog, Elastic, Commvault—tracking anomalies, ensuring data availability.
- **Data protectors**: Examples include Rubrik, NetApp, Varonis—specialists in backup, recovery and ransomware resilience.
- **Identity guardians**: Examples include CyberArk, Okta—securing the digital keys attackers covet.

Each slice of the stack lines up with the threats and regulations. Supply chain security mandates create demand for identity and monitoring. Ransomware pressures fuel adoption of backup and recovery. AI-driven threats magnify the need for edge filtering in real time. What looks like a fragmented vendor universe is, in fact, a map of how risks manifest.

Figure 1 notes the specific exposures within the WisdomTree Cybersecurity Fund (WCBR) of these particular firms.

Figure 1: WCBR Exposure across the Cybersecurity Ecosystem

Company Name	Weight	Area of Focus
Cloudflare Inc - Class A	5.0%	Edge Defenders
Akamai Technologies Inc	4.0%	Edge Defenders
Fastly Inc - Class A	3.4%	Edge Defenders
Zscaler Inc	5.0%	Network Security Leaders
Palo Alto Networks Inc	4.3%	Network Security Leaders
Fortinet Inc	4.3%	Network Security Leaders
Check Point Software Technolog	4.2%	Network Security Leaders
Crowdstrike Holdings Inc - A	5.6%	Endpoint Sentinels
Sentinelone Inc -Class A	5.1%	Endpoint Sentinels
Trend Micro Inc	4.2%	Endpoint Sentinels
Datadog Inc - Class A	4.9%	Observability & Resilience
Elastic Nv	4.1%	Observability & Resilience
CommVault Systems Inc	4.4%	Observability & Resilience
Rubrik Inc-A	4.3%	Data Protectors
Varonis Systems Inc	3.2%	Data Protectors
NetApp	0.0%	Data Protectors
Cyberark Software Ltd/Israel	5.1%	Identity Guardians
Okta Inc	4.1%	Identity Guardians

Source: WisdomTree, with data as of 9/22/25. **Holdings subject to change.**

Economics of Cybersecurity

From an economic lens, cybersecurity spending looks less like consumer tech and more like defense. It is countercyclical. Breaches trigger spending spikes. Regulation hardwires baseline demand. Geopolitical events reset urgency.

Verizon's 2025 report found that **attacks via third parties rose nearly 15% in a single year**. Each percentage point isn't abstract—it represents incremental procurement budgets, board-level urgency and software adoption curves. Marks & Spencer learned this the hard way in 2025, when an attack on a supplier spilled into its systems.[15]

That urgency explains why the global cybersecurity market—already $150 billion in 2022—is forecast to more than double by 2026.[16] This is not discretionary software. It is insurance for the digital economy.

Investor Dilemmas

But opportunity comes with complexity. Three dilemmas stand out:

- **Fragmentation vs. consolidation**: Enterprises often juggle dozens of tools. That creates inefficiency but also a chance for platforms like Palo Alto to consolidate. Specialists, however, remain critical in fast-evolving niches.
- **Regulatory divergence**: The EU and UK provide stable but costly growth. The U.S. is larger but unpredictable, oscillating between neglect and crisis-driven surges.
- **The paradox of success**: Cybersecurity works best when invisible. Success means breaches avoided—an absence that can make costs seem excessive until the next disaster validates them.

Investors have to think like insurers: pricing risk in a world where both regulation and criminal ingenuity are moving targets.

Closing: The Invisible Backbone

Cybersecurity is an invisible backbone of modern economies. It is national security when hospitals are locked. It is economic stability when customs systems go down. It is corporate strategy when boards weigh cloud migration. And it is investment when portfolios allocate capital to the firms building resilience.

The defining challenge of 2025 is that this backbone is under continuous strain. The weave between crime, state, policy and corporate defense is tight—and tightening. To understand cybersecurity, you cannot isolate the layers. You have to see the whole.

And seeing the whole reveals a truth that should shape strategy, policy and investment alike: cybersecurity is not simply protection. It is the infrastructure on which everything else depends.

Cybersecurity Awareness Month reinforces what 2025 makes clear: defense, policy and investment are converging. From boardrooms to battlefields, resilience isn't a side cost—it's the infrastructure that underpins growth, stability and innovation.

[1] Source: Associated Press, "Cyberattack causes disruption at major European airports, including Heathrow," Global News, 9/20/25.

[2] Source: "Cybercrime: A multifaceted national security threat (pp. 9–11)," Google Threat Intelligence Group, 2/25.

[3] Source: H. T. Neprash, E. McGlave, R. Lipton, M. Naylor and Kowalski, J. "Hacked to pieces? The effects of ransomware attacks on hospitals and patient outcomes," American Economic Review: Insights, Advance online publication, 2024.

[4] Source: "Cybercrime: A multifaceted national security threat" (pp. 7–11), Google Threat Intelligence Group, 2/25.

[5] An Initial Access Broker (IAB) is a cybercriminal who specializes in gaining unauthorized access to computer networks and then selling that access to other malicious actors

[6] Refers to North Atlantic Treaty Organization.

[7] GRU stands for Glavnoye Razvedyvatel'noye Upravleniye, which translates to the Main Intelligence Directorate. It was historically the foreign military intelligence agency of the General Staff of the Armed Forces of the Russian Federation.

[8] APT44 is the designation for the Russian state-sponsored cyber-sabotage unit also known as Sandworm.

[9] Source: "Cybercrime: A multifaceted national security threat" (pp. 14–20), Google Threat Intelligence Group, 2/25.

[10] Source: M. Negreiro, "The NIS2 Directive: A high common level of cybersecurity in the EU" (PE 689.333), European Parliamentary Research Service, 2023.

[11] Source: "Cyber Security and Resilience Policy Statement (CP 1299)," UK government, Department for Science, Innovation and Technology, 4/25.

[12] CISA stands for the Cybersecurity and Infrastructure Security Agency.

[13] Source: "Cyber Security and Resilience Policy Statement" (CP 1299), UK government, Department for Science, Innovation and Technology ,4/25.

[14] Source: "Cybercrime: A multifaceted national security threat" (pp. 10–11), Google Threat Intelligence Group, 2/25.

[15] Source: "2025 Data Breach Investigations Report" (pp. 15–16), Verizon Enterprise Solutions, 2025.

[16] Source: M. Negreiro, "The NIS2 Directive: A high common level of cybersecurity in the EU" (PE 689.333), European Parliamentary Research Service, 2023.

Important Risks Related to this Article

For current holdings of WCBR, please click here. Holdings are subject to risk and change.

There are risks associated with investing, including the possible loss of principal. The Fund invests in cybersecurity companies, which generate a meaningful part of their revenue from security protocols that prevent intrusion and attacks to systems, networks, applications, computers and mobile devices. Cybersecurity companies are particularly vulnerable to rapid changes in technology, rapid obsolescence of products and services, the loss of patent, copyright and trademark protections, government regulation and competition, both domestically and internationally. Cybersecurity company stocks, especially those that are internet-related, have experienced extreme price and volume fluctuations in the past that have often been unrelated to their operating performance. These companies may also be smaller and less experienced companies, with limited product or service lines, markets or financial resources and fewer experienced management or marketing personnel. The Fund invests in the securities included in, or representative of, its Index regardless of their investment merit, and the Fund does not attempt to outperform its Index or take defensive positions in declining markets. The composition of the Index is heavily dependent on quantitative and qualitative information and data from one or more third parties, and the Index may not perform as intended. Please read the Fund's prospectus for specific details regarding the Fund's risk profile.