Counter Cyberterrorism - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 122 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Counter Cyberterrorism Market size is estimated at USD 33.87 billion in 2025, and is expected to reach USD 39.76 billion by 2030, at a CAGR of 3.26% during the forecast period (2025-2030).

The Counter Cyberterrorism market is primarily driven by the growth in fear of cyberterrorism, which can impact a nation in several ways, leading to the deployment of cybersecurity solutions to prevent such attacks. Furthermore, the fear of attacks has increased significantly in the studied period, drawing the attention of state heads to building and deploying stronger and more secure solutions.

Key Highlights
- The digitalization of information & procedures and the increasing penetration of Internet platforms across the globe have increased the absolute risk of cyberterrorism. The increasingly interconnected world and the adoption of digital technologies and processes (IoT, cloud, mobile, big data, and artificial intelligence) in business and society have changed everyday life and revolutionized how they run.
- The rise in the connectivity of everything brings greater security, compliance, and data protection challenges and increases the absolute risk of cyberterrorism. Cybercriminals are also working on new methodologies to get through organizations' security and access everything from IP to individual customer information. This enhances the need for effective measures, thus driving the counter-cyberterrorism market.
- With the rise of next-generation features like application identification & control, firewall technology is evolving to become more flexible and secure. Moreover, the increase in firewalls is driven by the rising compliance guidelines and regulations to prevent external and internal threats. Also, due to the surge in real internal threats, users are now deploying firewalls in their internal networks, especially between switches, trust boundaries, and back-end servers. The market studied is anticipated to be driven by

increasing cyberterrorism and the rapid rise in data theft.
- In the Digital Defense Report (2022) by Microsoft, the organization identified the most common goals of major nation-state cyberattacks as espionage, disruption, and destruction. The most common methods were reconnaissance, credential harvesting, malware, and VPN exploitation. Tried and tested methods like large-scale spear-phishing campaigns are also valuable tools to hackers. According to the report, around 80% of nation-state-targeted attacks were on governments, NGOs, and think tanks. Attackers can utilize the connections between the NGO community & government organizations to understand national policy plans and intentions.
- Moreover, attacks on key infrastructures, such as power utilities, water treatment services, and health and emergency systems, are becoming more common and can have major consequences on operational performance.

Counter Cyberterrorism Market Trends

Growing Severity of Cyberattacks to Drive the Market

- Attacks on businesses, governments, and individuals have recently increased significantly. Infrastructure related to defense is fast becoming one of the most targeted choices among state-sponsored cyberattackers. Hence, these organizations have been acknowledging the value of disrupting the security systems that were previously considered impenetrable.
- Cyberattacks were introduced against Colonial Pipeline, the Massachusetts Steamship Authority, JBS (the world's largest meatpacker), and the Washington DC Metropolitan Police Department in 2022. These attacks on US organizations and firms had caused various key infrastructures to be shut down, resulting in shortages, higher prices of goods & services, and financial losses resulting from activities being halted.
- The increased adoption of machine-to-machine (M2M) technologies in the aerospace domain and the government's increasing focus on expanding cybersecurity to counter cyberterrorism have led to the cybersecurity market's growth over the past decade.
- The possible threat of cyberterrorism has sparked widespread concern. According to several security professionals, legislators, and others, cyberterrorists have hacked into government and commercial computer networks, crippling industrialized countries' financial, military, and service sectors.
- Moreover, the surge in data breaches throughout the globe acts as one of the key drivers for the counter-cyberterrorism market. Hence, the rising cases of data breaches will create various growth opportunities in the counter-cyberterrorism market. According to SurfShark, during the first quarter of 2022, worldwide Internet users saw approximately 18.1 million data breaches.

North America Accounts for Significant Market Share

- The United States is the most vital country targeted by cyberterrorism and countering such attacks. Moreover, the country also faces significant criticism from other nations for its state-sponsored cyber attacks; however, no such incident can fully claim the involvement of American security agencies or government in conducting such attacks.
- In February 2022, A Beijing-based cybersecurity firm accused the U.S. National Security Agency of creating a backdoor to spy on businesses and governments in more than 45 nations. According to a representative for China's Foreign Ministry, actions like this could jeopardize the security of China's essential infrastructure and compromise trade secrets.
- According to the United States Institute of Peace, even before 9/11, several exercises revealed apparent vulnerabilities in the military and energy industries' computer networks. Following 9/11, the security and terrorism narrative quickly shifted to include cyberterrorism, which interested political, corporate, and security actors encouraged.
- President Biden has made cybersecurity a high priority for the Biden-Harris Administration at all levels of government since it is a critical component of the Department of Homeland Security's (DHS) mission. In a virtual address hosted by the RSA Conference

in partnership with Hampton University and the Girl Scouts of the USA, Secretary Mayorkas outlined his broader vision and a roadmap for the Department's cybersecurity activities.
- In February 2023, The U.S. Marshals Service is investigating a significant ransomware attack that has compromised some of its most important information, including law enforcement materials, employees' personal information, and potential targets of federal investigations. The cyberattack was considered a "major incident" impacting a stand-alone system within the service.

Counter Cyberterrorism Industry Overview

The counter-cyberterrorism market is slightly competitive, owing to various players operating on a global scale. Some of the market's top players are Cisco Systems, Palo Alto Networks, and IBM Corporation.

In January 2023, The National Counter Ransomware Taskforce (NCRT) was introduced after the November All India Institute of Medical Science (AIIMS) attack. The central government worked on a task force to prevent such attacks in the future. The government was particularly concerned about cyber terrorism, cyber espionage, and ransomware, especially since the likely involvement of China and Pakistan has come to the name during investigations into the AIIMS attack.

In May 2022, Several Italian institutional websites, including the Italian Senate, the Ministry of Defense, and the National Institute of Health, were taken offline and unreachable for a few hours. This was a multiday cyber attack on day one, which targeted other Italian websites and other countries. The pro-Russian hacker groups Killnet and Legion claimed the attacks through their Telegram channels, killnet_channel and legion_russia. They used the Mirai malware to perform their DDoS (distributed denial-of-service) attacks on Italian websites.

In January 2022, The Belgian Defense Ministry detected a cyberattack and isolated the affected parts of its network. Belgium's Defense Ministry shut down parts of its computer network, including the ministry's mail system, for many days. The attackers used the Log4j vulnerability to gain access to the network.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

Counter Cyberterrorism - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 122 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-02-26
		Signature