

Cybersecurity Training Market Forecasts to 2034 – Global Analysis By Training Type (Technical Training, Awareness Training, Compliance Training, and Certification Training), Learning Mode (Classroom, Online, and Blended), Delivery Type, End User, Industry Vertical, and By Geography

<https://marketpublishers.com/r/C465B61F4A68EN.html>

Date: July 2026

Pages: 0

Price: US\$ 4,150.00 (Single User License)

ID: C465B61F4A68EN

Abstracts

According to Statistics MRC, the Global Cybersecurity Training Market is accounted for \$7.3 billion in 2026 and is expected to reach \$25.7 billion by 2034 growing at a CAGR of 16.9% during the forecast period. Cybersecurity training encompasses educational programs designed to develop skills, knowledge, and awareness related to protecting information systems, networks, and data from cyber threats. The market includes technical training for IT professionals, awareness training for general employees, compliance training for regulatory requirements, and certification training for professional credentials. These programs are delivered through classroom, online, and blended learning modes. Growing cyber threats, increasing regulatory requirements, rising data breaches, and the expanding cybersecurity skills gap are key drivers of market expansion. As organizations recognize employees as the first line of defense against cyber attacks, investment in cybersecurity training continues accelerating across all industry verticals.

Market Dynamics:

Driver:

Increasing frequency and sophistication of cyber attacks

The rising number and complexity of cyber attacks is a primary driver for the cybersecurity training market. Cyber threats including ransomware, phishing, social engineering, and advanced persistent threats are increasing in frequency and sophistication, targeting organizations across all sectors. Employees represent the most vulnerable attack surface, with human error accounting for a significant portion of security breaches. Organizations are investing in comprehensive training programs to reduce human vulnerability and build a security-aware culture. Regulatory mandates and insurance requirements are also driving training adoption. As the threat landscape continues evolving, ongoing employee education and skill development are essential for maintaining organizational security, sustaining strong market demand.

Restraint:

Budget constraints and limited training resources

Limited cybersecurity training budgets and resource constraints represent significant restraints for market growth. Many organizations, particularly small and medium enterprises, struggle to allocate sufficient funding for comprehensive training programs. Cybersecurity training competes with other business priorities for limited resources. The need for ongoing, regular training creates recurring costs that strain budgets. Employee time away from core responsibilities represents an opportunity cost. Developing and updating training content requires specialized expertise and ongoing investment. In developing regions, resource limitations restrict program availability. These cost and resource constraints limit training program scope and frequency, affecting market penetration.

Opportunity:

Integration of gamification and immersive learning technologies

The integration of gamification and immersive learning technologies presents significant opportunities for cybersecurity training market expansion. Gamification elements including points, badges, leaderboards, and competitions enhance learner engagement and motivation. Interactive simulations, virtual labs, and scenario-based training provide hands-on experience in safe environments. Virtual and augmented reality technologies create immersive training experiences that improve retention and skill transfer. Microlearning modules delivered through mobile platforms support just-in-time learning and reinforcement. As organizations seek more engaging, effective training approaches, gamified and immersive solutions are gaining adoption, creating new growth avenues.

Threat:

Rapid evolution of cyber threats and training content obsolescence

The rapid evolution of cyber threats and resulting training content obsolescence pose significant threats to the cybersecurity training market. Attack techniques and defense strategies evolve continuously, requiring frequent content updates to remain relevant. Developing and maintaining up-to-date training materials requires significant investment and specialized expertise. Organizations may hesitate to invest in training programs that could become outdated quickly. The challenge of balancing foundational skills with emerging threat awareness creates complexity. This content obsolescence pressure may lead organizations to favor shorter, more agile training formats and cloud-based platforms with continuous updates.

Covid-19 Impact:

The COVID-19 pandemic significantly accelerated cybersecurity training adoption as remote work expanded attack surfaces and increased security risks. Organizations rapidly deployed security awareness training for remote employees, addressing new threats including phishing, home network vulnerabilities, and secure collaboration practices. The shift to remote learning accelerated online training platform adoption, with many classroom programs transitioning to virtual delivery. Budget pressures in some sectors affected training investment, but increased cyber threat awareness reinforced training importance. Post-pandemic, hybrid work models sustain elevated cybersecurity training demand, with ongoing focus on remote workforce security.

The Technical Training segment is expected to be the largest during the forecast period

The Technical Training segment is expected to account for the largest market share during the forecast period, driven by the growing demand for skilled cybersecurity professionals and the need for specialized technical skills across organizations. Technical training includes courses on network security, ethical hacking, incident response, security operations, cloud security, and secure coding. The segment benefits from the widening cybersecurity skills gap, with organizations struggling to find qualified professionals. Certification preparation programs support professional development and credentialing. Government initiatives promoting cybersecurity workforce development drive program expansion. As organizations invest in building technical capabilities, technical training maintains the largest market share.

The Online segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the Online segment is predicted to witness the highest growth rate, fueled by the scalability, accessibility, and cost-effectiveness of digital training delivery. Online training eliminates geographic barriers, enabling organizations to reach distributed workforces. Self-paced learning accommodates varied schedules and learning preferences, improving completion rates. Video-based content, interactive modules, and virtual labs provide engaging learning experiences. Learning management systems enable tracking, reporting, and compliance verification. Mobile compatibility supports learning on any device. As remote and hybrid work persist and technology platforms advance, online cybersecurity training delivers the fastest segment growth.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, supported by strong cybersecurity awareness, significant enterprise security investment, and established training infrastructure. The United States leads global cybersecurity spending, with organizations across sectors prioritizing security training. Regulatory requirements including HIPAA, PCI DSS, and state privacy laws mandate security awareness training, driving consistent demand. Strong presence of training providers, certification bodies, and security vendors supports market growth. Government cybersecurity initiatives and workforce development programs further accelerate adoption. With regulatory drivers and established training culture, North America maintains its dominant market position.

Region with highest CAGR:

Over the forecast period, the Asia-Pacific region is anticipated to exhibit the highest CAGR, driven by rapid digital transformation, increasing cyber threats, and growing awareness of cybersecurity importance. Countries including India, China, Australia, and Singapore are experiencing expanding cybersecurity training investment as organizations build security capabilities. Government cybersecurity strategies and regulatory frameworks are driving training requirements. The region's large and growing technology workforce creates substantial demand for professional training. Rising cyber attack frequency across the region is increasing awareness. As digital transformation accelerates and security priorities rise, Asia Pacific delivers the fastest cybersecurity training market growth globally.

Key players in the market

Some of the key players in Quantum Communication Market include SANS Institute, EC-Council, CompTIA, Inc., OffSec Services Limited, Infosec Institute, Inc., Fortinet, Inc., Cisco Systems, Inc., Palo Alto Networks, Inc., Check Point Software Technologies Ltd., Proofpoint, Inc., Trend Micro Incorporated, Firebrand Training Limited, QA Limited, Learning Tree International, Inc., Global Knowledge Training LLC, Koenig Solutions Pvt. Ltd., Skillsoft Corporation, and INE, Inc.

Key Developments:

In June 2026, Fortinet faced a major global credential exposure campaign dubbed 'FortiBleed,' prompting formal security alerts from CISA and international security units urging organizations to immediately terminate active SSL VPN sessions and harden up to 74,000 internet-facing FortiGate firewall gateways.

In March 2026, the SANS Institute delivered its prominent 'Top 5 Most Dangerous New Attack Techniques' briefing at RSAC 2026, alongside the rollout of specialized technical work frameworks addressing complex multi-vector threats and advanced cryptographic defense.

In January 2026, CompTIA released its IT Industry Outlook 2026 study, revealing that 94% of surveyed technology professionals intend to explicitly invest in specialized AI and data security architectures to counter increasingly complex automated digital environments.

Training Types Covered:

Technical Training

Awareness Training

Compliance Training

Certification Training

Learning Modes Covered:

Classroom

Online

Blended

Delivery Types Covered:

Self-Paced

Instructor-Led

Virtual Labs

End Users Covered:

Individuals

Enterprises

Government

Educational Institutions

Industry Verticals Covered:

BFSI

Healthcare

Government

IT and Telecommunications

Manufacturing

Retail

Energy and Utilities

Other Industry Verticals

Regions Covered:

North America

United States

Canada

Mexico

Europe

United Kingdom

Germany

France

Italy

Spain

Netherlands

Belgium

Sweden

Switzerland

Poland

Rest of Europe

Asia Pacific

China

Japan

India

South Korea

Australia

Indonesia

Thailand

Malaysia

Singapore

Vietnam

Rest of Asia Pacific

South America

Brazil

Argentina

Colombia

Chile

Peru

Rest of South America

Rest of the World (RoW)

Middle East

Saudi Arabia

United Arab Emirates

Qatar

Israel

Rest of Middle East

Africa

South Africa

Egypt

Morocco

Rest of Africa

What our report offers:

Market share assessments for the regional and country-level segments

Strategic recommendations for the new entrants

Covers Market data for the years 2023, 2024, 2025, 2026, 2027, 2028, 2030, 2032 and 2034

Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)

Strategic recommendations in key business segments based on the market

estimations

Competitive landscaping mapping the key common trends

Company profiling with detailed strategies, financials, and recent developments

Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

Contents

1 EXECUTIVE SUMMARY

- 1.1 Market Snapshot and Key Highlights
- 1.2 Growth Drivers, Challenges, and Opportunities
- 1.3 Competitive Landscape Overview
- 1.4 Strategic Insights and Recommendations

2 RESEARCH FRAMEWORK

- 2.1 Study Objectives and Scope
- 2.2 Stakeholder Analysis
- 2.3 Research Assumptions and Limitations
- 2.4 Research Methodology
 - 2.4.1 Data Collection (Primary and Secondary)
 - 2.4.2 Data Modeling and Estimation Techniques
 - 2.4.3 Data Validation and Triangulation
 - 2.4.4 Analytical and Forecasting Approach

3 MARKET DYNAMICS AND TREND ANALYSIS

- 3.1 Market Definition and Structure
- 3.2 Key Market Drivers
- 3.3 Market Restraints and Challenges
- 3.4 Growth Opportunities and Investment Hotspots
- 3.5 Industry Threats and Risk Assessment
- 3.6 Technology and Innovation Landscape
- 3.7 Emerging and High-Growth Markets
- 3.8 Regulatory and Policy Environment
- 3.9 Impact of COVID-19 and Recovery Outlook

4 COMPETITIVE AND STRATEGIC ASSESSMENT

- 4.1 Porter's Five Forces Analysis
 - 4.1.1 Supplier Bargaining Power
 - 4.1.2 Buyer Bargaining Power
 - 4.1.3 Threat of Substitutes
 - 4.1.4 Threat of New Entrants

- 4.1.5 Competitive Rivalry
- 4.2 Market Share Analysis of Key Players
- 4.3 Product Benchmarking and Performance Comparison

5 GLOBAL CYBERSECURITY TRAINING MARKET, BY TRAINING TYPE

- 5.1 Technical Training
- 5.2 Awareness Training
- 5.3 Compliance Training
- 5.4 Certification Training

6 GLOBAL CYBERSECURITY TRAINING MARKET, BY LEARNING MODE

- 6.1 Classroom
- 6.2 Online
- 6.3 Blended

7 GLOBAL CYBERSECURITY TRAINING MARKET, BY DELIVERY TYPE

- 7.1 Self-Paced
- 7.2 Instructor-Led
- 7.3 Virtual Labs

8 GLOBAL CYBERSECURITY TRAINING MARKET, BY END USER

- 8.1 Individuals
- 8.2 Enterprises
- 8.3 Government
- 8.4 Educational Institutions

9 GLOBAL CYBERSECURITY TRAINING MARKET, BY INDUSTRY VERTICAL

- 9.1 BFSI
- 9.2 Healthcare
- 9.3 Government
- 9.4 IT and Telecommunications
- 9.5 Manufacturing
- 9.6 Retail
- 9.7 Energy and Utilities

9.8 Other Industry Verticals

10 GLOBAL CYBERSECURITY TRAINING MARKET, BY GEOGRAPHY

10.1 North America

10.1.1 United States

10.1.2 Canada

10.1.3 Mexico

10.2 Europe

10.2.1 United Kingdom

10.2.2 Germany

10.2.3 France

10.2.4 Italy

10.2.5 Spain

10.2.6 Netherlands

10.2.7 Belgium

10.2.8 Sweden

10.2.9 Switzerland

10.2.10 Poland

10.2.11 Rest of Europe

10.3 Asia Pacific

10.3.1 China

10.3.2 Japan

10.3.3 India

10.3.4 South Korea

10.3.5 Australia

10.3.6 Indonesia

10.3.7 Thailand

10.3.8 Malaysia

10.3.9 Singapore

10.3.10 Vietnam

10.3.11 Rest of Asia Pacific

10.4 South America

10.4.1 Brazil

10.4.2 Argentina

10.4.3 Colombia

10.4.4 Chile

10.4.5 Peru

10.4.6 Rest of South America

10.5 Rest of the World (RoW)

10.5.1 Middle East

10.5.1.1 Saudi Arabia

10.5.1.2 United Arab Emirates

10.5.1.3 Qatar

10.5.1.4 Israel

10.5.1.5 Rest of Middle East

10.5.2 Africa

10.5.2.1 South Africa

10.5.2.2 Egypt

10.5.2.3 Morocco

10.5.2.4 Rest of Africa

11 STRATEGIC MARKET INTELLIGENCE

11.1 Industry Value Network and Supply Chain Assessment

11.2 White-Space and Opportunity Mapping

11.3 Product Evolution and Market Life Cycle Analysis

11.4 Channel, Distributor, and Go-to-Market Assessment

12 INDUSTRY DEVELOPMENTS AND STRATEGIC INITIATIVES

12.1 Mergers and Acquisitions

12.2 Partnerships, Alliances, and Joint Ventures

12.3 New Product Launches and Certifications

12.4 Capacity Expansion and Investments

12.5 Other Strategic Initiatives

13 COMPANY PROFILES

13.1 SANS Institute

13.2 EC-Council

13.3 CompTIA, Inc.

13.4 OffSec Services Limited

13.5 Infosec Institute, Inc.

13.6 Fortinet, Inc.

13.7 Cisco Systems, Inc.

13.8 Palo Alto Networks, Inc.

13.9 Check Point Software Technologies Ltd.

- 13.10 Proofpoint, Inc.
- 13.11 Trend Micro Incorporated
- 13.12 Firebrand Training Limited
- 13.13 QA Limited
- 13.14 Learning Tree International, Inc.
- 13.15 Global Knowledge Training LLC
- 13.16 Koenig Solutions Pvt. Ltd.
- 13.17 Skillsoft Corporation
- 13.18 INE, Inc.

List Of Tables

LIST OF TABLES

Table 1 Global Cybersecurity Training Market Outlook, By Region (2023–2034) (\$MN)

Table 2 Global Cybersecurity Training Market Outlook, By Training Type (2023–2034) (\$MN)

Table 3 Global Cybersecurity Training Market Outlook, By Technical Training (2023–2034) (\$MN)

Table 4 Global Cybersecurity Training Market Outlook, By Awareness Training (2023–2034) (\$MN)

Table 5 Global Cybersecurity Training Market Outlook, By Compliance Training (2023–2034) (\$MN)

Table 6 Global Cybersecurity Training Market Outlook, By Certification Training (2023–2034) (\$MN)

Table 7 Global Cybersecurity Training Market Outlook, By Learning Mode (2023–2034) (\$MN)

Table 8 Global Cybersecurity Training Market Outlook, By Classroom (2023–2034) (\$MN)

Table 9 Global Cybersecurity Training Market Outlook, By Online (2023–2034) (\$MN)

Table 10 Global Cybersecurity Training Market Outlook, By Blended (2023–2034) (\$MN)

Table 11 Global Cybersecurity Training Market Outlook, By Delivery Type (2023–2034) (\$MN)

Table 12 Global Cybersecurity Training Market Outlook, By Self-Paced (2023–2034) (\$MN)

Table 13 Global Cybersecurity Training Market Outlook, By Instructor-Led (2023–2034) (\$MN)

Table 14 Global Cybersecurity Training Market Outlook, By Virtual Labs (2023–2034) (\$MN)

Table 15 Global Cybersecurity Training Market Outlook, By End User (2023–2034) (\$MN)

Table 16 Global Cybersecurity Training Market Outlook, By Individuals (2023–2034) (\$MN)

Table 17 Global Cybersecurity Training Market Outlook, By Enterprises (2023–2034) (\$MN)

Table 18 Global Cybersecurity Training Market Outlook, By Government (2023–2034) (\$MN)

Table 19 Global Cybersecurity Training Market Outlook, By Educational Institutions

(2023–2034) (\$MN)

Table 20 Global Cybersecurity Training Market Outlook, By Industry Vertical

(2023–2034) (\$MN)

Table 21 Global Cybersecurity Training Market Outlook, By BFSI (2023–2034) (\$MN)

Table 22 Global Cybersecurity Training Market Outlook, By Healthcare (2023–2034) (\$MN)

Table 23 Global Cybersecurity Training Market Outlook, By Government (2023–2034) (\$MN)

Table 24 Global Cybersecurity Training Market Outlook, By IT and Telecommunications (2023–2034) (\$MN)

Table 25 Global Cybersecurity Training Market Outlook, By Manufacturing (2023–2034) (\$MN)

Table 26 Global Cybersecurity Training Market Outlook, By Retail (2023–2034) (\$MN)

Table 27 Global Cybersecurity Training Market Outlook, By Energy and Utilities (2023–2034) (\$MN)

Table 28 Global Cybersecurity Training Market Outlook, By Other Industry Verticals (2023–2034) (\$MN)

Note: Tables for North America, Europe, APAC, South America, and Rest of the World (RoW) Regions are also represented in the same manner as above.

I would like to order

Product name: Cybersecurity Training Market Forecasts to 2034 – Global Analysis By Training Type (Technical Training, Awareness Training, Compliance Training, and Certification Training), Learning Mode (Classroom, Online, and Blended), Delivery Type, End User, Industry Vertical, and By Geography

Product link: <https://marketpublishers.com/r/C465B61F4A68EN.html>

Price: US\$ 4,150.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/C465B61F4A68EN.html>