

Cybersecurity Trends Report



Presented by eTeam's Workforce Intelligence Team  WIT

The **United States** is seeing increased interest in cybersecurity careers driven by several statistical factors:

Competitive Salaries and Benefits: Cybersecurity roles continue to offer lucrative financial incentives. According to the 2024 Cybersecurity Salary Survey by ISC2, the **median salary** for cybersecurity professionals in the US is approximately **\$112,000** annually.

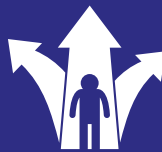
Diverse Career Opportunities: A report from Burning Glass Technologies in 2024 indicates that roles such as information security analysts, cybersecurity engineers, and penetration testers have experienced a **32% growth** in job postings, highlighting extensive opportunities for specialization.

Significant Workforce Impact: As per the 2024 Data Breach Report by Verizon, cybersecurity efforts have mitigated **over 60%** of potential data breaches, demonstrating the critical role professionals play in protecting digital assets.

Key Factors



COMPETITIVE
SALARIES

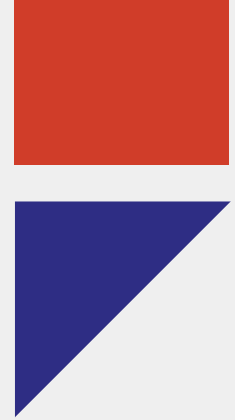


DIVERSE
OPPORTUNITIES



WORKFORCE
IMPACT





Key Skills in Demand

Cybersecurity roles require a strong foundation in specific technical skills:

Proficiency in Cybersecurity Tools: Expertise in tools like Wireshark, Metasploit, and SIEM (Security Information and Event Management) systems.

Programming Languages: Languages such as Python, Java, and emerging languages like Rust are highly valued.

Network Security: Skills in setting up firewalls, Intrusion Detection Systems (IDS), and Virtual Private Networks (VPNs).

Key Threats Addressed

Cybersecurity professionals are tasked with countering a range of sophisticated threats:

Ransomware and Malware Attacks

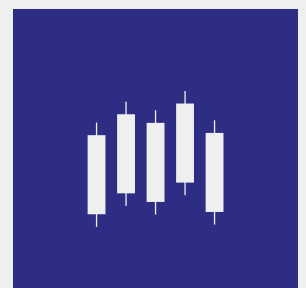
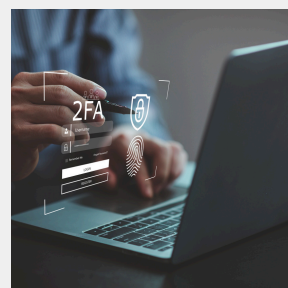
As noted in the CompTIA study, these remain the predominant threats faced by US organizations.

Phishing Schemes

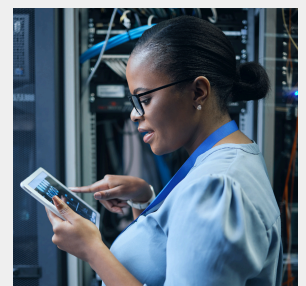
Enhanced social engineering tactics require vigilance and continuous training to prevent breaches.

IoT Vulnerabilities

The expanding Internet of Things presents new security challenges due to the sheer number of connected devices.



Cybersecurity roles are projected to expand due to increasing cyber threats





Projected Growth



From 2023 to 2025

30%–35%



**\$300 Bn
by 2026**

The cybersecurity sector is set for significant growth, with emerging areas such as cloud security, AI-enhanced cybersecurity, and zero-trust architecture anticipated to drive demand for skilled professionals

BUREAU OF LABOR STATISTICS

The Bureau of Labor Statistics predicts that information security analyst roles will grow by **35% from 2023 to 2025**, much faster than the average for all occupations.

CYBERSECURITY VENTURES

According to Cybersecurity Ventures, global cybersecurity spending is expected to reach **\$300 billion** by 2026, illustrating the growing importance of securing digital assets.



Conclusion

As businesses and governments continue to prioritize cybersecurity, the demand for skilled professionals will only grow. By attracting, developing, and retaining top talent in the field, the United States can enhance its cybersecurity posture and safeguard its digital future.



REPORT PRESENTED BY:



FOR MORE INFORMATION



+123-456-7890



www.eteaminc.com



amaggio@eteaminc.com