

McKinsey  
& Company

# MassVision2050

Cybersecurity

December 2025

MASSACHUSETTS  
**HIGHTECHNOLOGYCOUNCIL**

*Dedicated to Growth... Committed to Action*

CONFIDENTIAL AND PROPRIETARY  
Any use of this material without specific permission of McKinsey & Company  
is strictly prohibited



---

# Definition of Cybersecurity

The practice of protecting systems, networks, and data from cyber threats through technologies, processes, and policies. The cybersecurity industry is a rapidly growing sector focused on safeguarding digital assets across all industries, driven by increasing threats and a global shortage of skilled professionals.

---

---

## Approach to quantifying market share and economic competitiveness:

- Analyze locations of companies with significant investments in cybersecurity
- Investigate patents held on cybersecurity topics and where the owners of those patents are located
- Aggregate job postings and professional profiles that use keywords related to cybersecurity:
  - Cybersecurity, information security, network security, cloud security, penetration testing, threat intelligence, security operations center (SOC)
- Review VC investment in cybersecurity across MA and the rest of the US
- Identify notable startups and exits in the space

# Executive Summary: Cybersecurity

Preliminary

## Macro trends

- The Cybersecurity market is estimated to be worth ~\$200B and is expected to grow at ~12% CAGR through 2027, with an anticipated additional 12%+ in growth driven by artificial intelligence and cloud adoption
- Expected growth drivers for the industry include continued increases in enterprise-level digitalization (e.g., migration to the cloud), and a new shift towards AI security awareness and prompt engineering
- Cyber hubs in the US are centered around established tech ecosystems, e.g., California, Texas, and New York (top 3 states for cybersecurity workforce), and government cybersecurity hubs, e.g., Virginia (5<sup>th</sup>), Maryland (9<sup>th</sup>), and Washington D.C. (11<sup>th</sup>)
- MA ranks 14<sup>th</sup> among leading states in its cybersecurity workforce population, accounting for 2.5% of all cybersecurity-related profiles

## Talent Supply and Demand

- MA ranks 10<sup>th</sup> among US states for new cybersecurity-related jobs with over 8K postings in 2025
- There has been an increase in demand for Cybersecurity jobs in MA and nationally (17% growth in MA, 7% in US since 2021) with more employers competing for talent; on average, it takes employers ~9% longer to fill a cyber role today than it did in 2021
- MA has experienced 9% growth in university completions for cybersecurity related programs in 2024, with Northeastern, Worcester Polytechnic Institute, and MIT having the highest share of total completions
- The specific skillsets in demand are shifting, with rapid growth in disaster risk and compliance related skills such as disaster recovery, HIPPA compliance, incidence response as well as increasing demand for emerging technologies and AI skills

## Startup and Investment Landscape

- NSF funding for cybersecurity-related R&D has remained stable over the last few years (MA currently has \$24M in active grants, up from \$23M in 2023), with Northeastern and Worcester Polytechnic Institute leading in R&D funding awards
- Cybersecurity is the 12<sup>th</sup> highest funded vertical for venture capital investment in MA over the past 5 years, attracting \$4.5B in funding over the last 5 years, accounting for 9% of cybersecurity VC funding in the US

---

# Objectives for today

- **Macro trends and dynamics**
- Talent supply and demand
- Startup and investment landscape

# The industry is divided between organizations that are pure play providers and those for which cyber is an organizational function

Each industry segment has a different chain across which value in cybersecurity is derived

Preliminary

■ Details to follow

Organizations with business and operating models dedicated to providing cybersecurity products and services to other organizations, e.g., cyber resilience products providers, IoT security services consultants



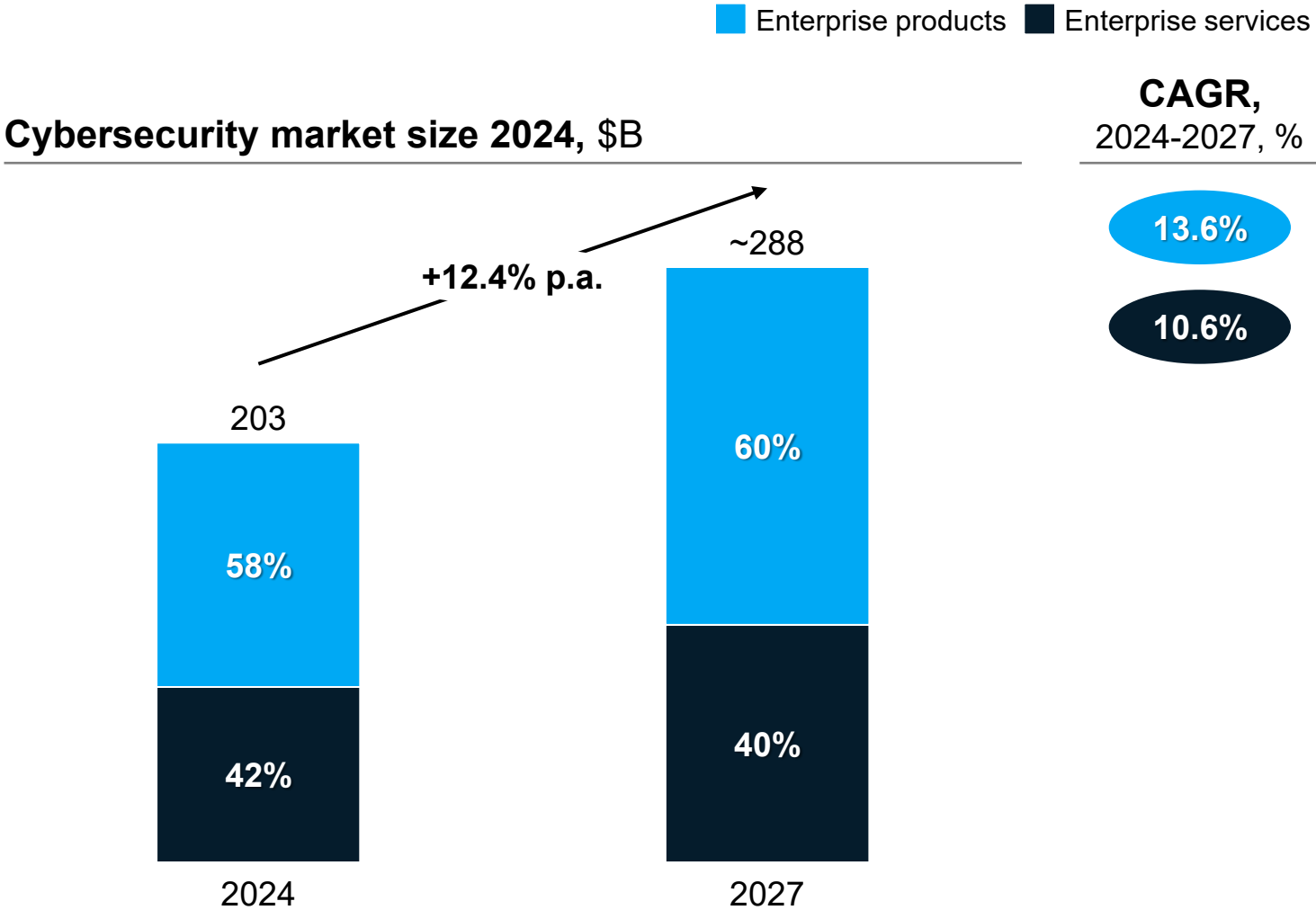
**Pure play  
cybersec.  
providers**



**Cyber as  
an industry  
function**

Organizations for which cybersecurity is a necessary and critical function for their operating model, e.g., CISOs at organizations in financial services, the public sector, life sciences / healthcare, broader technology, entertainment

# The ~200B cybersecurity market is growing resiliently with 12+% CAGR



1. 2017-2020 CAGR ~10%, 2020-2023 CAGR ~12.5%

## Key takeaways

Cyber market is **resilient** and **growing at steady pace** since years<sup>1</sup>

**12+% secular tailwinds** driven by **AI** and **cloud** adoption

**High willingness to pay** given high number of **breaches** across industry and strict **regulation** (e.g., DORA)

# A: The overall market for cyber providers can be divided into 13 segments across enterprise products and 3<sup>rd</sup>-party services (1/2)

Preliminary

Segment	Description	● Products	● Services
<b>1 Endpoint protection</b>	Provide advanced protection of endpoints (desktops, laptops, smartphones, tablets) as well as detection / response to threats targeting them		
<b>2 Network security</b>	Prevent attackers from gaining access to a company's network and infrastructure through NGFW, IPS/IDS, VPN etc.		
<b>3 Identity and access management</b>	Provide tools and governance model/ processes to control access to information across employees, customers, contractors, and applications		
<b>4 Security Operations</b>	Assess current risk, maturity, and vulnerabilities and manage a full spectrum of security operations (esp. threat detection and response)		
<b>5 Email security and awareness</b>	Protect email and collaboration apps (extensible into instant messaging (IM)) through URL filtering, content filtering, phishing protection / awareness		
<b>6 Web security</b>	Protect against both inbound (malware) and outbound (data leakage) threats related to web applications		
<b>7 IoT/OT security<sup>1</sup></b>	An emerging market for security of factories and other manufacturing/ industrial facilities with multiple nodes, as well as of individual IoT devices		

# A: The overall market for cyber providers can be divided into 13 segments across enterprise products and 3<sup>rd</sup>-party services (2/2)

Preliminary

Segment	Description	● Products	● Services
8 <b>GRC &amp; IRM solutions<sup>1</sup></b>	Support organization's processes around governance, integrated risk management, policy and compliance	●	●
9 <b>Managed Security Services (MSS)</b>	Security Operations Center functions outsourced as a managed services contract, including monitoring (L1-L3+), event management, threat intelligence, incident response	●	●
10 <b>Consulting</b>	Services ranging from helping to design solutions, implementation phase as well as outsourcing and follow-on support	●	●
11 <b>Cloud Security</b>	Tools to harden configurations, control permissions, broker access, and protect workloads actively running in the cloud	●	●
12 <b>Application Security</b>	Tools to help developers quickly and painlessly build, test, and verify code they write are secure / adhere to security policies	●	●
13 <b>Data protection</b>	Suites to ensure data at rest is stored in a secure manner, accessed, and transacted upon only in allowable ways by authorized parties	●	●

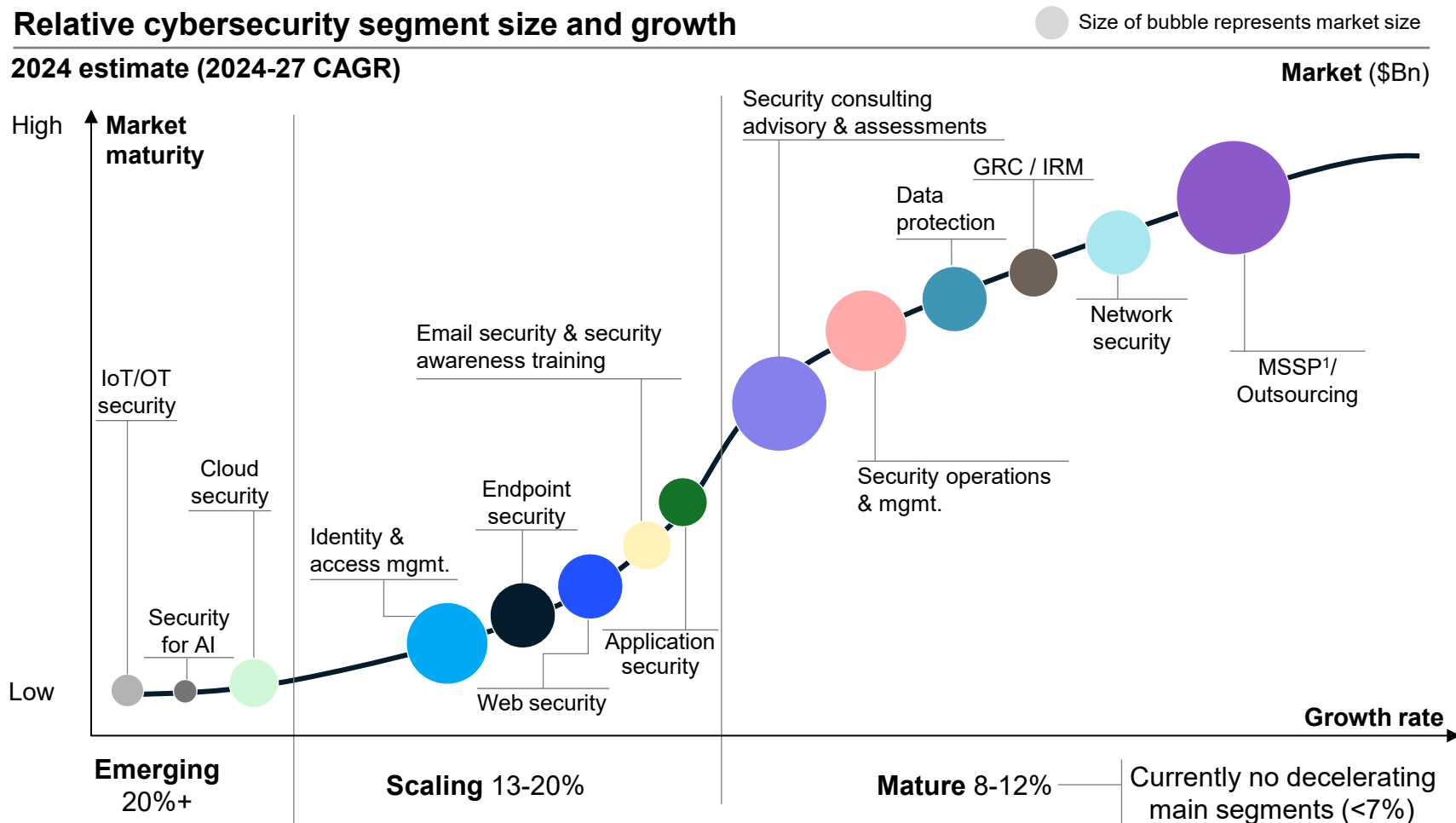
# Within that ~\$200B market, segments are moving at varying speeds based on maturity

Overall market CAGR for 2024-27 is 12.4%

Illustrative

## Relative cybersecurity segment size and growth

2024 estimate (2024-27 CAGR)



1. Excludes implementation



**IoT/OT, cloud, and AI security are emerging** and experience strong growth with 20%+ CAGR

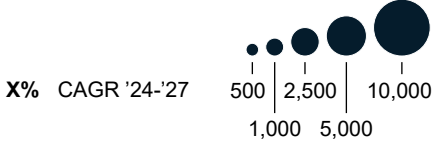
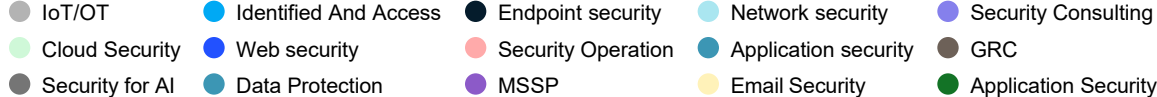


**Traditional segments** such as **network, GRC, and MSSP** are considered table stakes and entering maturity on growth curve

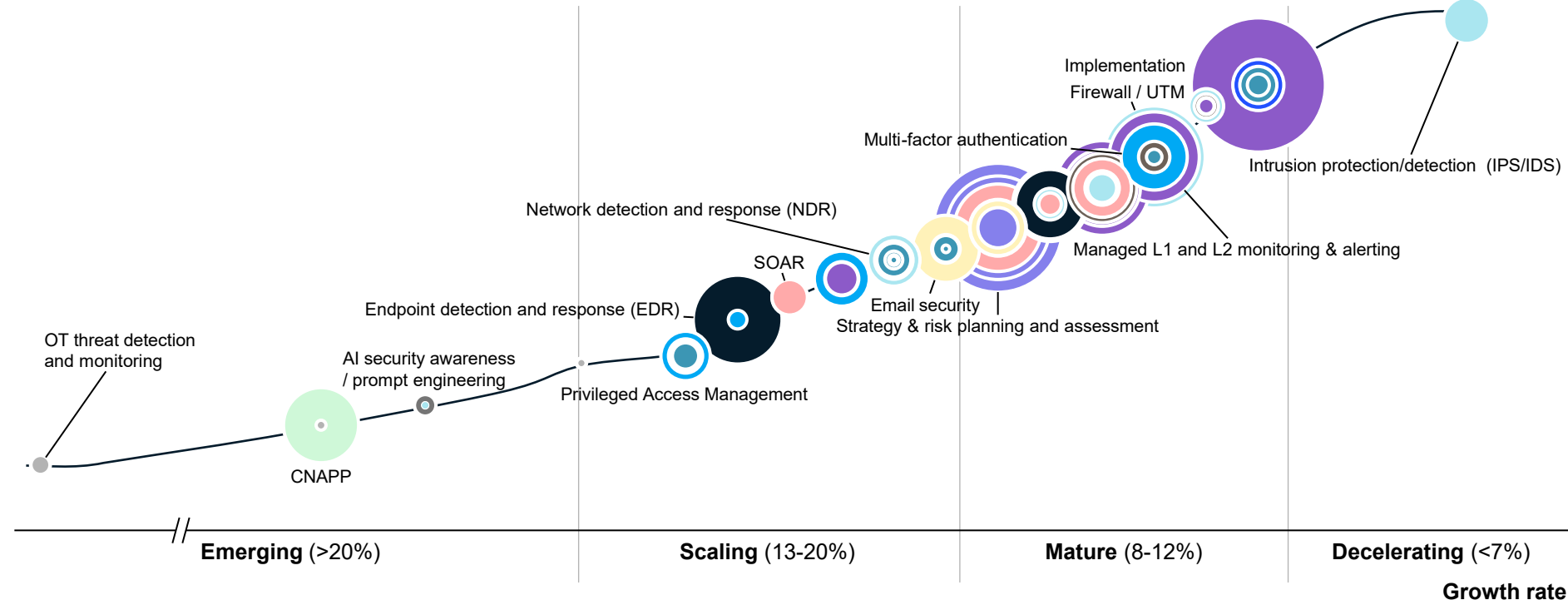
# The market can be further segmented, and has yet to choose a winner in certain high growth value pools (i.e., 20%+)

**Illustrative**

**Relative cybersecurity segment size and growth<sup>1</sup>**



**Fluidity in market definition**



**Key insights**

Key market subsegments with a >20% CAGR:

- **Cloud security with CNAPP** platforms (combining former CSPM and CWPP solutions)
- **OT security: Secure network access, threat detection and monitoring, and services** (MDR, MSSP, 24/7 Monitoring), driven by convergence of IT and OT
- **Security for AI**, with model governance, firewalls, prompt engineering training

Providers should expect to see more customer/seller activities (e.g., roll-up/consolidation)

1. Currently excludes Hardware security modules (HSM), Cyber deception / honeypots and Mobile device protection as team is still working on the market estimates

# A: These six selected trends are shaping the overall near-term cybersecurity market for providers

Preliminary



**1**

**Growth of hybrid and multi-cloud**

Multi-cloud and hybrid environments are increasing in complexity, with a purely “cloud-native” world still far off for enterprises



**2**

**Increased acceptance of SaaS cyber**

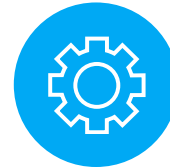
Usage of SaaS cybersecurity solution is anticipated to accelerate by 10%+ over the coming 3 years



**3**

**Regulatory pressure and splinternet**

Countries are increasingly developing data privacy, protection and localization regulations to which companies must adapt their operations



**4**

**Automation and DevOps**

Digitization is expanding log volumes which requires additional capacity and automation to parse effectively, while agile developers face increased security responsibilities



**5**

**From Protect to Detect and Respond**

An increasing number of attack surfaces (e.g., IoT devices) and attackers is increasing the remit of the security organization



**6**

**Cyber market is consolidating**

Cybersecurity market may have reached a “post-peak” trough in new company formation – # of new cyber companies formed slowing down post 2018 while M&A deals are on a rise

# The industry is divided between organizations that are pure play providers and those for which cyber is an organizational function

Each part of the industry has a different chain across which value in cybersecurity is derived

Preliminary

■ Details to follow

Organizations with business and operating models dedicated to providing cybersecurity products and services to other organizations, e.g., cyber resilience products providers, IoT security services consultants



**Pure play  
cybersec.  
providers**



**Cyber as  
an industry  
function**

Organizations across many industries for which cybersecurity is a necessary and critical function for their operating model, e.g., CISOs at organizations in financial services, the public sector, life sciences / healthcare, broader technology, entertainment

# B: For organizations that use cyber, i.e., non-providers, the value chain can be better categorized into 8 capabilities...

Preliminary

2 Governance, Risk, and Compliance

4 Architecture and Engineering

6 Cyber Resilience and Recovery

8 Physical Security and Safety



1 Strategy, Program Management, & Performance

3 Identity and Access Management

5 Security Operations and Response

7 Data Protection and Privacy

# B: The cybersecurity attack surface grows with increasing digitization, connectivity and migration to cloud

Preliminary

## 1 Information Technology (IT) / Operational Technology (OT)

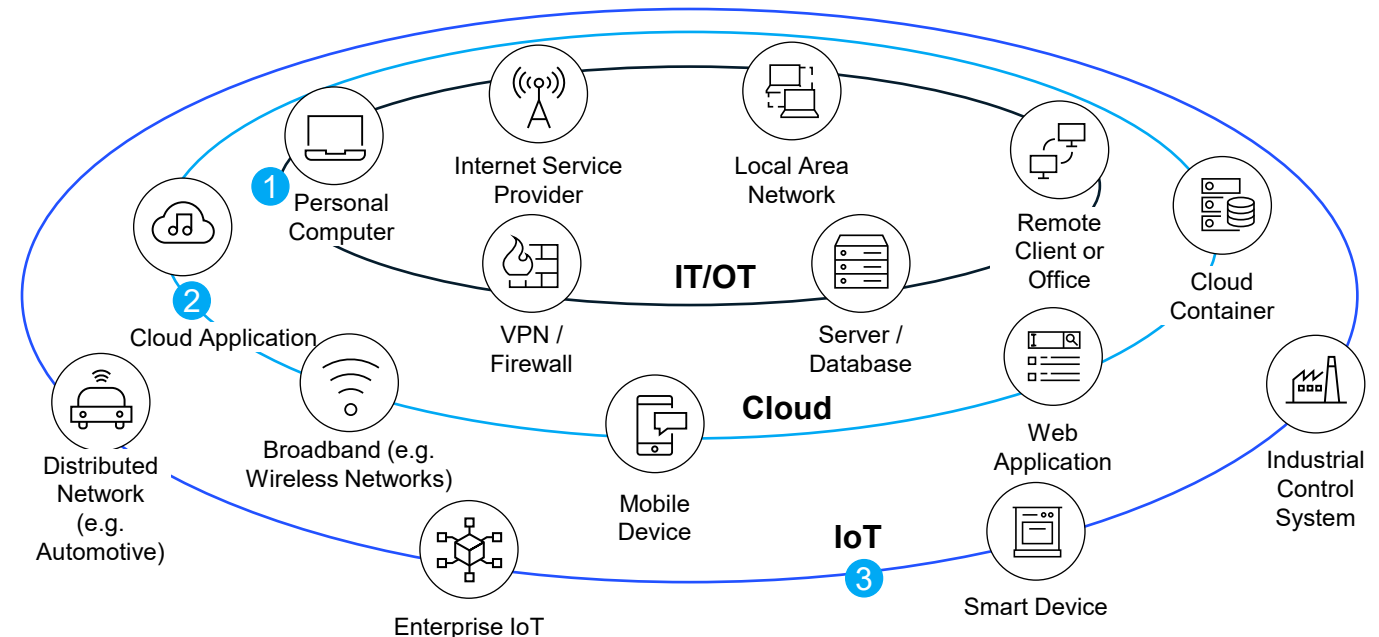
IT / OT includes all corporate owned and managed systems, including both computers and machinery.

## 2 Cloud / External Supplier systems

Security and privacy introduce unique challenges as cloud providers often have responsibility for maintenance and operation of security controls

## 3 Internet of Things (IoT)

Internet of things are systems of interconnected computing devices which communicate with one another without the need for human interaction.



**Attack surface** refers to the sum of systems and applications that can be exploited to carry out a cybersecurity attack. **One method of reducing the impact of a cyber-attack** is to reduce the attack surface of a given system or organization.

# MA ranks 14<sup>th</sup> in size of its cybersecurity workforce

Preliminary

Rank	State	Cybersecurity workforce <sup>1</sup>	% of total workforce <sup>2</sup>
1	California	102,918	10.4
2	Texas	89,155	9.0
3	New York	61,931	6.3
4	Florida	53,752	5.5
5	Virginia	44,753	4.5
6	Georgia	35,920	3.6
7	North Carolina	31,064	3.2
8	Illinois	30,671	3.1
9	Maryland	29,864	3.0
10	Washington	28,564	2.9
11	District of Columbia	27,400	2.8
12	Pennsylvania	25,279	2.6
13	Colorado	24,593	2.5
14	Massachusetts	24,364	2.5
15	Ohio	20,623	2.0

1. Profile Analytics using cybersecurity-related keywords, profiles updated since 2018; 2. % of total cybersecurity-related profiles

---

# Objectives for today

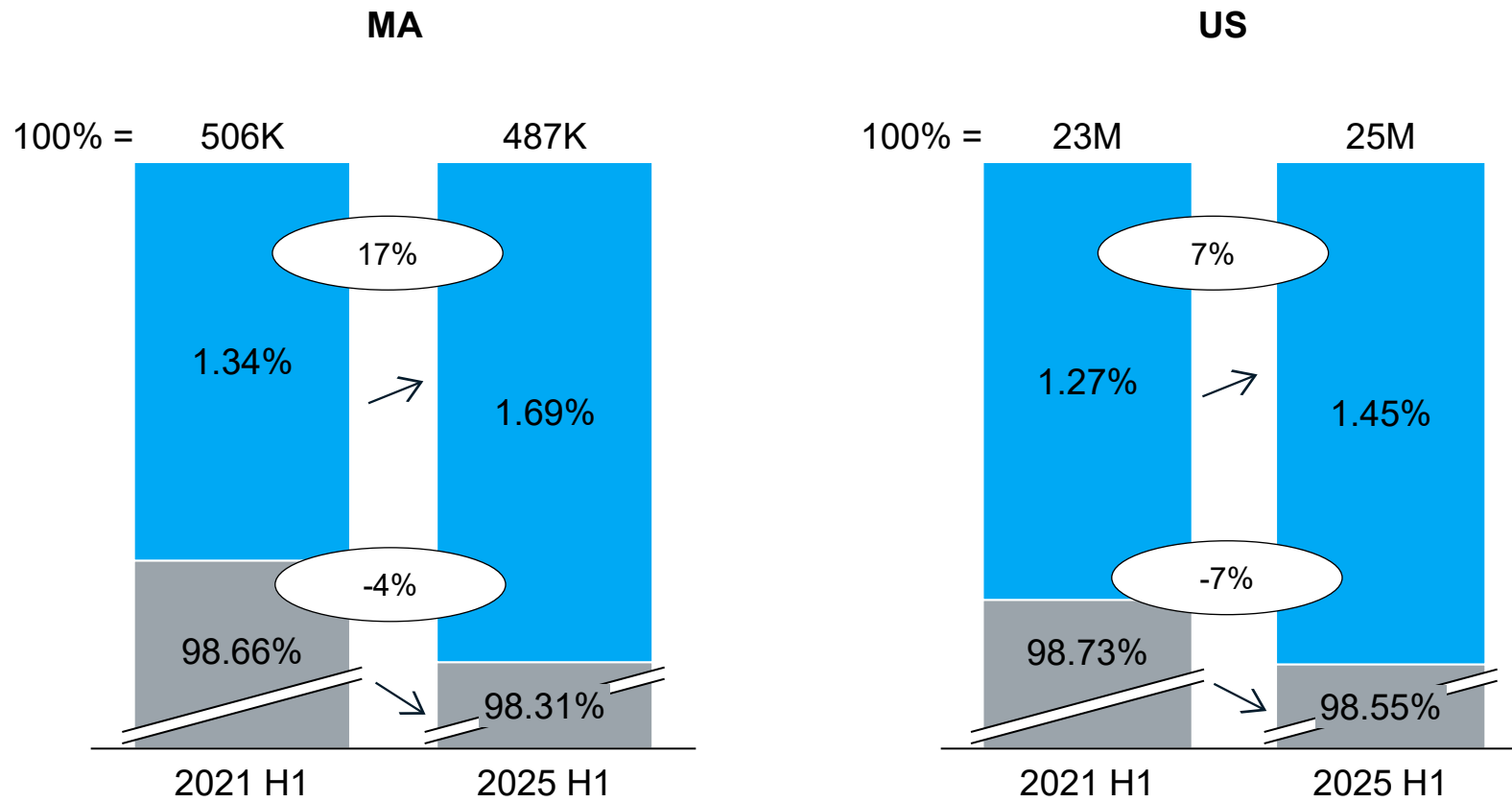
- Macro trends and dynamics
- **Talent supply and demand**
- Startup and investment landscape

# Nearly 2% of job postings in MA are for Cybersecurity jobs; postings have increased since 2021 H1 in both MA and the US

Preliminary

Share of total postings<sup>1</sup>, %  
Postings for jobs using cybersecurity-related keywords<sup>2</sup>

■ Cybersecurity postings ■ Rest of postings  
○ % growth



- Currently, Cybersecurity job postings make up ~1.7% of postings in MA and ~1.5% in the US overall
- Cybersecurity postings have increased since 2021 H1 in both MA and the US, though MA has seen a larger increase (17% vs 7%)
- While cybersecurity postings have increased, overall job postings have decreased slightly from 2021 H1 to 2025 H1

1. De-duplicated job postings, or online vacancies, scraped from over 45,000 websites, including company career sites, national and local job boards, and job posting aggregators  
2. Keywords include: cybersecurity, information security, network security, cloud security, penetration testing, threat intelligence, and security operations center (SOC)

# Massachusetts is among the top states for Cybersecurity postings, but ranks 28<sup>th</sup> overall for posting growth

Preliminary

## Top 15 states ranked by number of Cybersecurity-related postings

Postings for jobs using cybersecurity-related keywords<sup>1</sup>

State	Postings, K, 2025 H1	% of region's postings	Growth, 2021H1-2025H1
California	24.7	1.4%	-12%
Texas	22.6	1.5%	-24%
Virginia	22.5	4.1%	17%
New York	11.7	1.3%	15%
Maryland	11.1	3.7%	30%
Florida	10.8	1.0%	4%
Pennsylvania	9.5	1.4%	16%
Illinois	9.3	1.4%	19%
Georgia	8.9	1.7%	2%
<b>Massachusetts</b>	<b>8.2</b>	<b>1.7%</b>	<b>17%</b>
Colorado	8.1	1.9%	-26%
North Carolina	7.2	1.2%	-13%
Ohio	6.8	1.0%	26%
Arizona	6.2	1.6%	-13%
District of Columbia	6.1	6.1%	-21%
US total	252.8	1.5%	7%

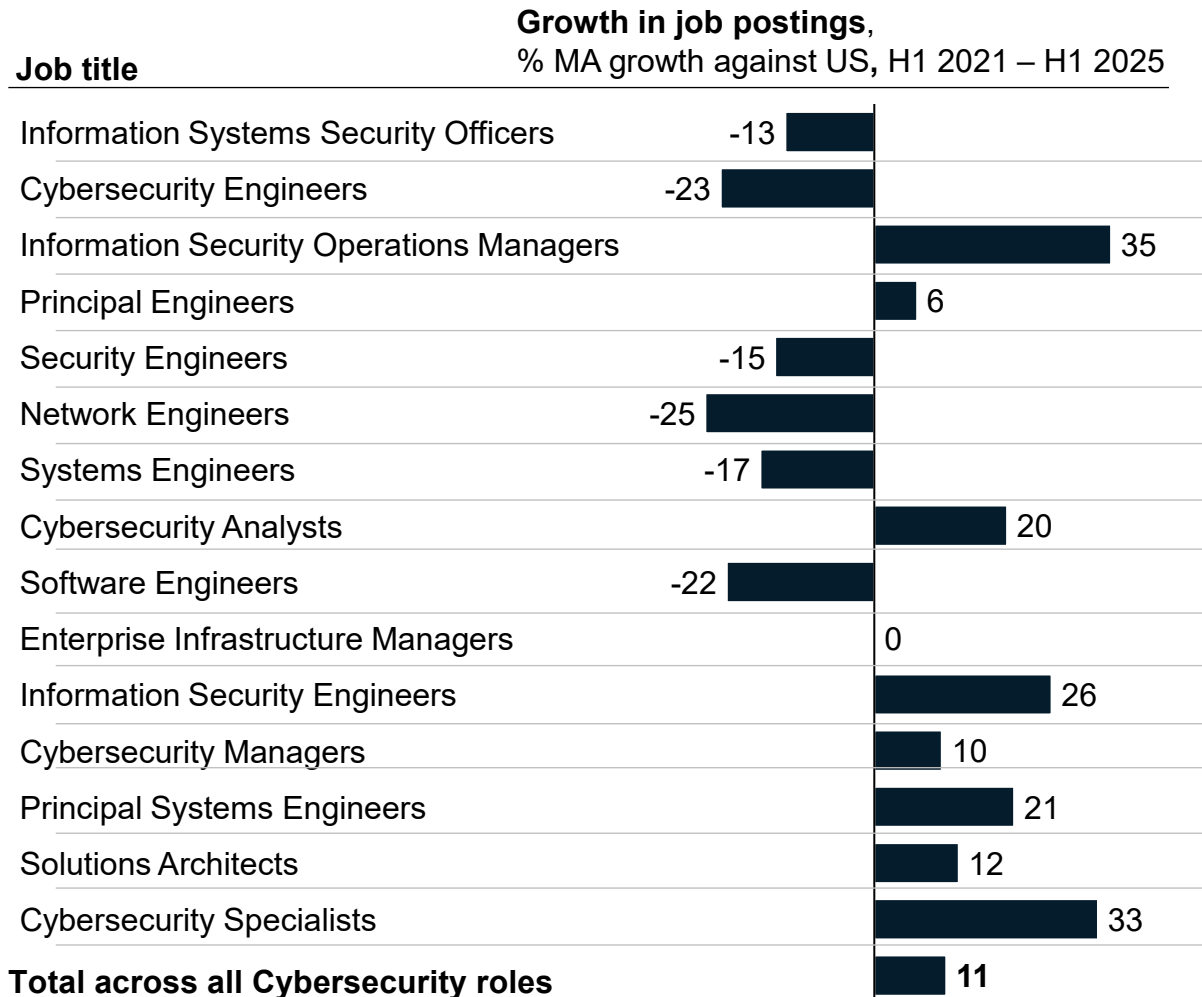
- MA had the 10<sup>th</sup> highest number of Cybersecurity postings in the first half of 2025
- Cybersecurity postings make up a small share of overall postings across all states in the top 15, with the highest shares in DC, VA, and MD
- Job postings in some of the top states, e.g., CA and TX, have decreased since 2021

1. Keywords include: cybersecurity, information security, network security, cloud security, penetration testing, threat intelligence, and security operations center (SOC)

# Relative to the US, demand for manager roles increased in MA while demand for certain engineering roles decreased

Preliminary

## Top 15 roles by number of postings for jobs using cybersecurity-keywords<sup>1</sup>



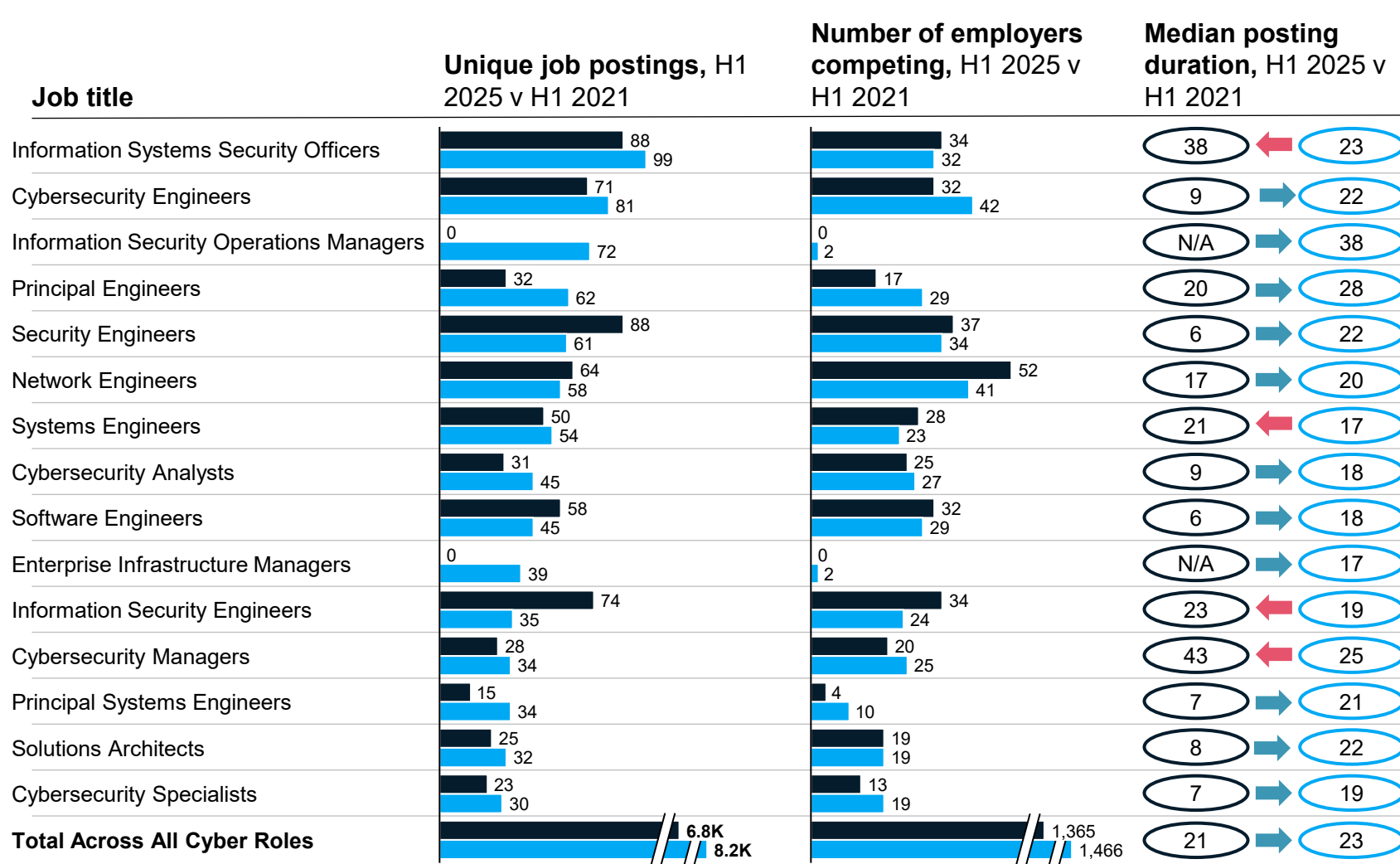
- Demand for Cybersecurity jobs in MA grew by ~17% since 2021, while nationally demand only increased by ~7%
- **Change in demand for Cybersecurity roles has differed in MA** compared to the US overall:
  - Demand for Information Security Operations Managers, Cybersecurity Specialists, and Information Security Engineers grew substantially more in MA than the US overall
  - Demand for Network Engineers, Cybersecurity Engineers, and Software Engineers grew less in MA than the US as a whole

1. Keywords include: cybersecurity, information security, network security, cloud security, penetration testing, threat intelligence, and security operations center (SOC)

# Job postings for Cybersecurity roles have increased, as have number of employers competing; postings today take ~9% longer to fill

Top 15 roles by number of postings for jobs using cybersecurity-related keywords in MA

**Preliminary**



- Cybersecurity job postings increased from 6.8K in H1 2021 to 8.2K in H1 2025
- The number of employers competing for Cybersecurity talent has increased from ~1.4K in H1 2021 to ~1.5K employers in H1 2025
- Roles are becoming harder for employers to fill: median posting duration is 23 days (compared to 21 in 2021), with the highest increases for security, software, and principal systems engineer postings

# Based on online profile data, ~24K MA-based workers work in cybersecurity related roles or have cybersecurity skills

Top 15 states ranked by number of cybersecurity-related profiles<sup>1</sup>

Preliminary

State	Online profiles, K	% of region's profiles	% of cybersecurity profiles nationally
California	102.9	0.6%	12.3%
Texas	89.2	0.7%	10.6%
New York	61.9	0.6%	7.4%
Florida	53.8	0.5%	6.4%
Virginia	44.8	1.2%	5.3%
Georgia	35.9	0.7%	4.3%
North Carolina	31.1	0.7%	3.7%
Illinois	30.7	0.5%	3.7%
Maryland	29.9	1.1%	3.6%
Washington	28.6	0.8%	3.4%
District of Columbia	27.4	2.2%	3.3%
Pennsylvania	25.3	0.5%	3.0%
Colorado	24.6	0.8%	2.9%
<b>Massachusetts</b>	<b>24.4</b>	<b>0.6%</b>	<b>2.9%</b>
Ohio	20.6	0.4%	2.5%
<b>US total</b>	<b>837.5</b>		

- **Massachusetts ranks 14<sup>th</sup>** in number of cybersecurity profiles, accounting for 2.9% of total cybersecurity profiles in the US
- **DC, VA, and MD have the largest concentration of cybersecurity-related skills** or occupations (2.2%, 1.2%, and 1.1% respectively)

1. Data scraped from individual profiles of over 144M workers in the US, sources are proprietary to Lightcast

# MA is producing sufficient talent to fill the top Cybersecurity-related roles

Preliminary

## Top in-demand occupations within the cybersecurity sector in MA

■ <50% Completions relative to Openings
 ■ 51% - 75% Completions relative to Openings
 ■ 75%+ Completions relative to Openings

Occupations	All MA job postings, Thousands, 2025	Completions <sup>1</sup> , 2024	Typical entry level education
Computer Occupations, All Other	2.0	2020	Bachelor's degree
Software Developers	0.5	4576	Bachelor's degree
Computer Network Architects	0.3	324	Bachelor's degree
Information Security Analysts	0.3	605	Bachelor's degree
Computer User Support Specialists	0.2	3232	Some college, no degree
Marketing Managers	0.2	1013	Bachelor's degree
Managers, All Other	0.2	13368	Bachelor's degree
Network and Computer Systems Administrators	0.2	404	Bachelor's degree
Computer and Information Systems Managers	0.2	2526	Bachelor's degree
Data Scientists	0.2	716	Bachelor's degree
General and Operations Managers	0.1	9003	Bachelor's degree
Architectural and Engineering Managers	0.1	4296	Bachelor's degree
Financial Risk Specialists	0.1	56	Bachelor's degree
Industrial Engineers	0.1	201	Bachelor's degree
Postsecondary Teachers	0.1	380	Doctoral or professional degree
Financial Managers	0.1	1828	Bachelor's degree

- General computer occupations are in highest demand in MA with local graduates accounting for more than 75% of the demand for job openings in the state
- MA seems to have a good supply of graduates for some roles, but sees lower levels of completions for financial risk specialists and industrial engineers
- Most of the cybersecurity occupations require at least a bachelor's degree, excluding computer user support specialists

1. Completions in 2024 (the most recent data available) are used as a proxy for the level of 2025 graduates (as 2025 are not yet released). To adjust for duplication, the number of completions within each degree program (CIP) was distributed to each corresponding occupation (SOC) typically requiring a four-year degree or higher by way of a weighted average based on current employment within occupations

\*Except technical and scientific products

# Massachusetts universities produced ~7K graduates in Cybersecurity-related fields in 2023

Preliminary

## Completions in Cybersecurity and related programs<sup>1</sup>, 2023

Top 15 MA universities, by number of completions

		% of total completions	Growth, 2018-2023 CAGR	Retention rate <sup>2</sup>
Northeastern University	1,503	15%	25%	41.4%
University of Massachusetts-Amherst	817	8%	17%	39.7%
Massachusetts Institute of Technology	745	18%	3%	19.1%
Boston University	559	4%	15%	32.7%
Worcester Polytechnic Institute	317	15%	9%	42.5%
Harvard University	307	3%	-2%	18.9%
Tufts University	295	6%	9%	33.1%
University of Massachusetts-Lowell	288	6%	10%	47.2%
Boston College	184	4%	21%	30.0%
University of Massachusetts-Boston	145	4%	7%	48.6%
Wentworth Institute of Technology	145	15%	6%	45.1%
Brandeis University	140	6%	-2%	31.4%
Fitchburg State University	120	7%	23%	40.9%
University of Massachusetts-Dartmouth	76	4%	-7%	63.9%
Wellesley College	67	9%	3%	28.0%
<b>Total</b>	<b>6,715</b>	<b>5%</b>	<b>9%</b>	<b>42.6%</b>

- Specialized Cybersecurity related degrees include: Computer and Information Systems Security/Auditing/Information Assurance and Homeland Security
- While cybersecurity-related programs have generally seen growth in MA, Harvard, Brandeis, and UMass Dartmouth have seen a decline in completions
- Graduate retention rate is below state average for many of the top universities graduating Cybersecurity-related talent

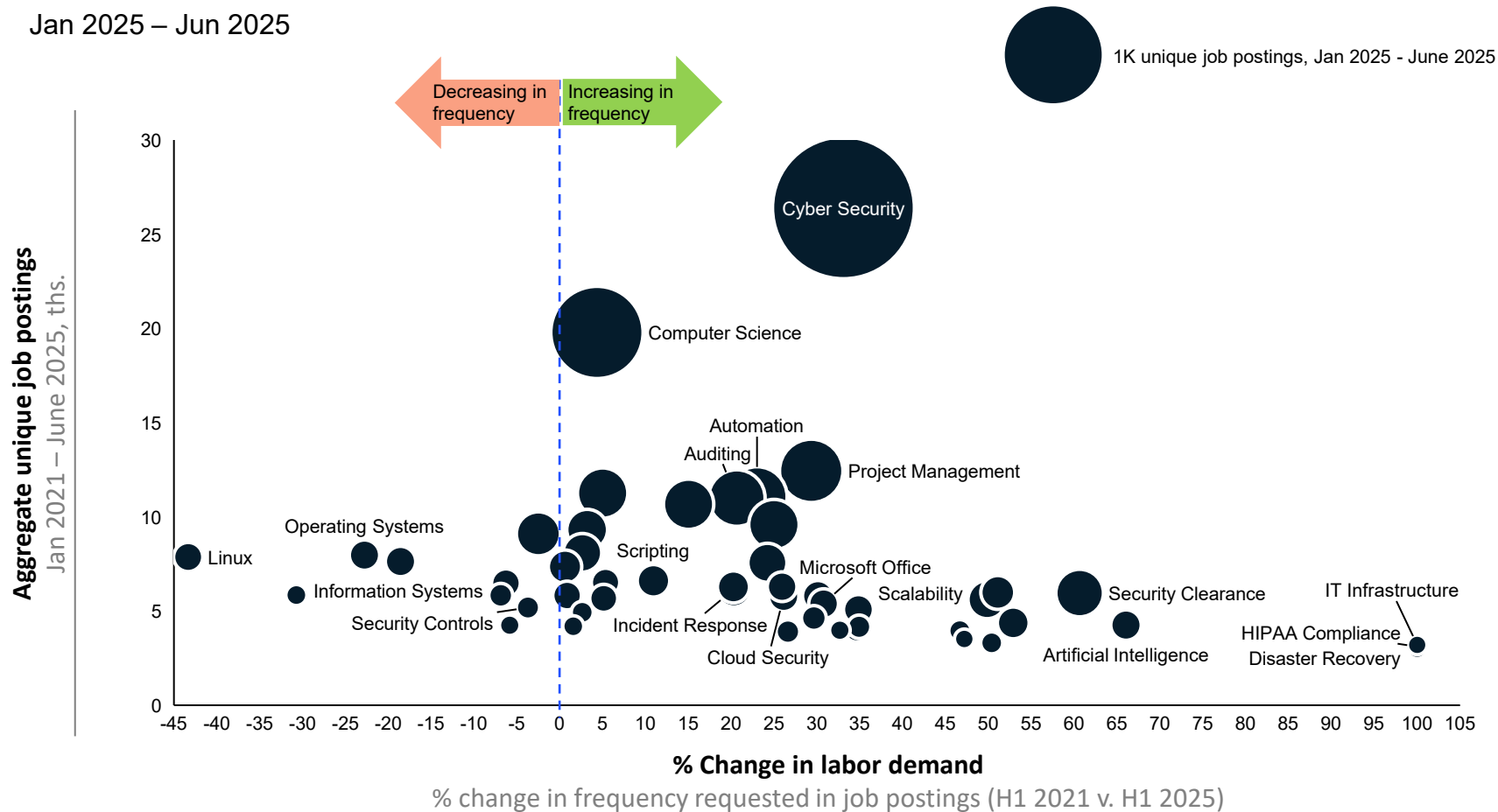
1. CIP codes: Computer Science (11.0701), Computer and Information Sciences, General (11.0101), Computer Systems Networking and Telecommunications (11.0901), Computer and Information Systems Security/Auditing/Information Assurance (11.1003), Computer/Computer Systems Technology/Technician (15.1202), Homeland Security (43.0301) 2. Overall university retention rate, not program specific

# Demand for risk assessment-related skills grew substantially since 2021 for Cybersecurity jobs

Preliminary

## Top 50 in-demand hard-skills<sup>1</sup> for MA employers in the Cybersecurity sector

Jan 2025 – Jun 2025



- Demand for skills like IT Infrastructure, Disaster Recovery and HIPAA Compliance appeared in the years since 2021, indicating a shift in focus on cybersecurity job postings
- Demand has declined for foundational computing skills, such as operating and information systems, software engineering, and Linux

1. Based on job postings filtered by cybersecurity-related keywords in MA. Specialized, software, and certificate skills only (excludes common skills)

# Raytheon has been seeking the most Cybersecurity talent in the past year, but demand is spread across a range of companies and industries

**Preliminary**

MA companies	MA job postings, Unique postings, 2025	% of postings
Raytheon Technologies	746	9.1%
Arinc International Of Canada Ulc	341	4.2%
Schneider Electric	275	3.3%
State Street Corporation	195	2.4%
MITRE Corporation	186	2.3%
Highmark Health	108	1.3%
Mastercard	104	1.3%
Point32Health	102	1.2%
Lumen Technologies	95	1.2%
Bristol Community College	95	1.2%
Cyberark	69	0.8%
Ropes & Gray LLP	65	0.8%
Oracle	62	0.8%
Rapid7	61	0.7%
Amazon	60	0.7%
Total MA Postings	8,212	

- The top 15 companies seeking Cybersecurity talent account for ~31% of postings for these roles, but there were over 8K companies seeking Cybersecurity talent over the past year
- There are a variety of industries represented among top companies seeking Cybersecurity talent: aerospace and defense, healthcare, banking/finance, R&D, consulting, telecommunication

---

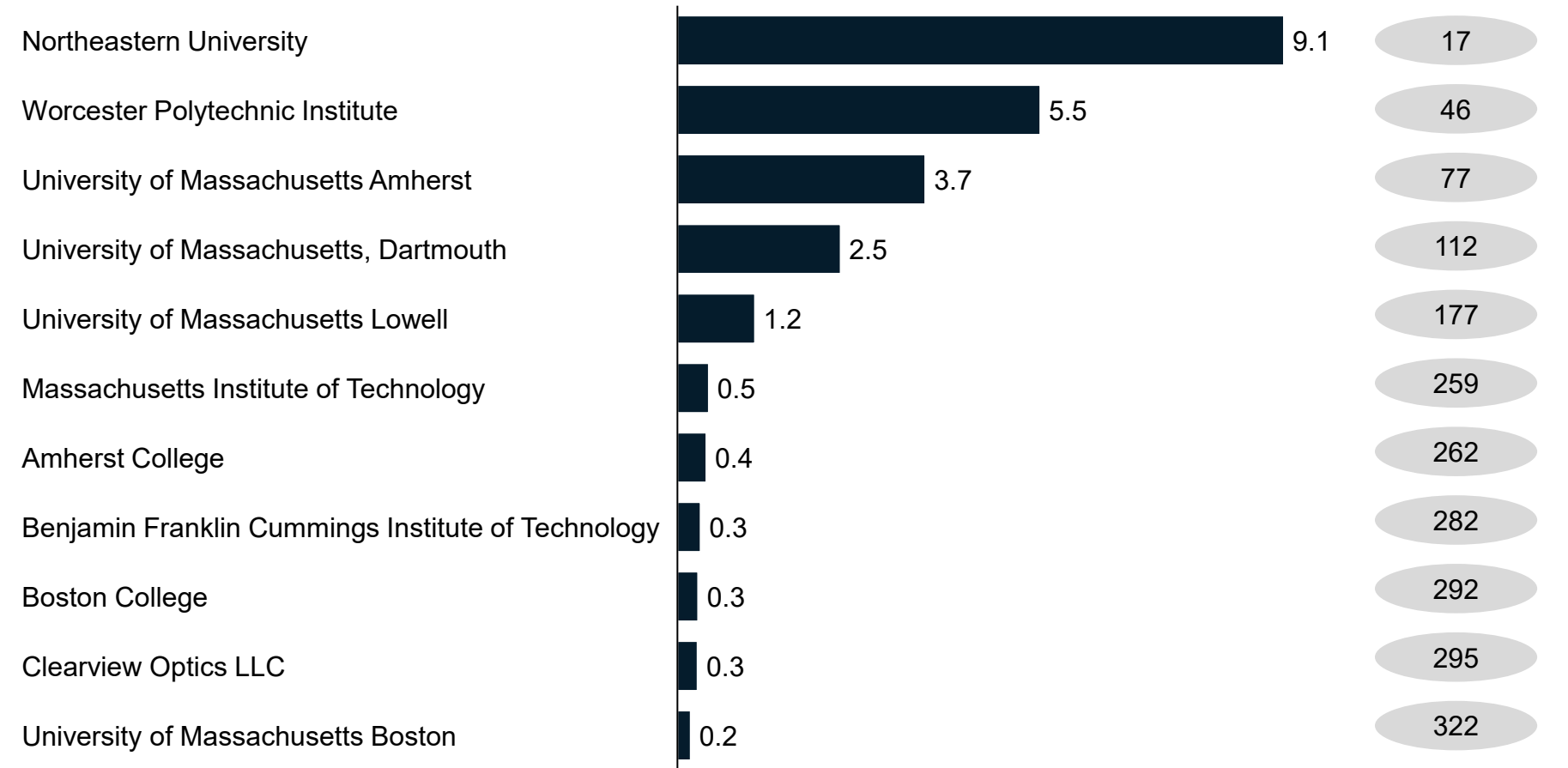
# Objectives for today

- Macro trends and dynamics
- Talent supply and demand
- **Startup and investment landscape**

# Northeastern and Worcester Polytechnic Institute lead the state's Cybersecurity R&D funding from the NSF

Preliminary

Cybersecurity-related R&D funding from NSF, by institution  
Active awards as of August 2025, \$M

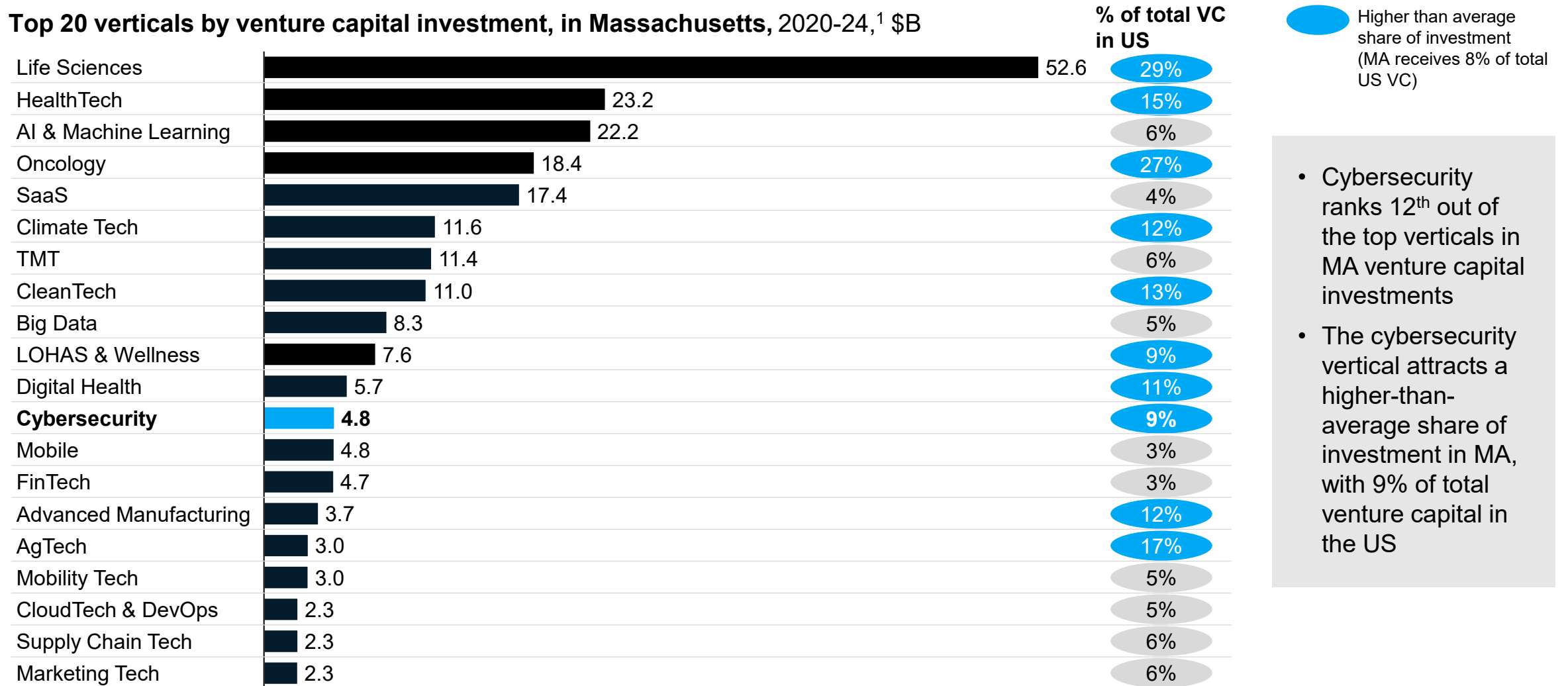


- 11 MA institutions and research organizations have active NSF grants for Cybersecurity R&D, totaling over \$24M in funding (compared to 13 institutions receiving \$23M in funding in 2023)
- National leaders in Cybersecurity R&D include: University of Illinois (#1), Arizona State University (#2), and University of Southern California (#3)

1. Among 358 institutions in the US with active awards

# Cybersecurity has the 12<sup>th</sup> highest vertical by venture capital investment, with a higher-than-average share of investment in MA

Top 20 verticals by venture capital investment, in Massachusetts, 2020-24,<sup>1</sup> \$B



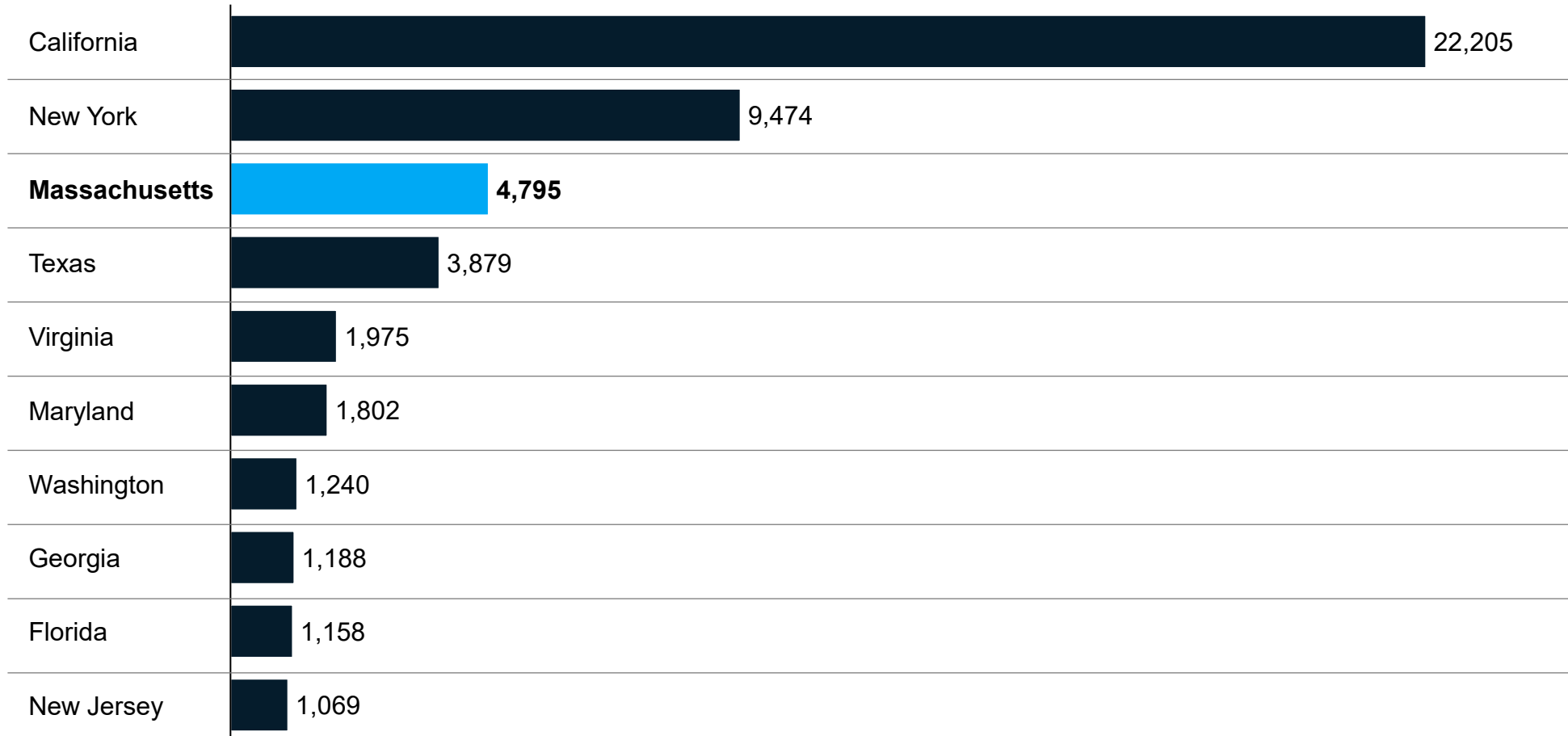
- Cybersecurity ranks 12<sup>th</sup> out of the top verticals in MA venture capital investments
- The cybersecurity vertical attracts a higher-than-average share of investment in MA, with 9% of total venture capital in the US

1. Figures will not sum up to total as multiple tech verticals can be applied to one deal; removed high-level verticals that include other verticals such as "Manufacturing" and "Industrials"

# California leads states in Cybersecurity VC investment by a wide margin; MA attracts the 3<sup>rd</sup> most Cybersecurity VC nationally

Preliminary

Top 10 states for Cybersecurity VC investment, 2020-24, \$, Million



- California leads in AI VC investment nationally, attracting over 2x the investment of the next highest state, New York
- Massachusetts ranks 3<sup>rd</sup> nationally for Cybersecurity VC investment, attracting just under half New York's VC investment

# There has been 1 cybersecurity startup valued over \$1B in MA over the last 5 years

~37

Cybersecurity early-stage startups active<sup>1</sup> in MA

0

IPO in the past 5 years

29

M&A exits in the past 5 years

1. Active startups defined as: Privately held, PE, VC, or accelerator/incubator, or angel backed with business status generating revenue, product development or startup

Preliminary

## Top 10 transactions by deal size, Cybersecurity startups, 2020-2024

Company	Exit type	Exit date	Approx. valuation, \$M
Recorded Future	M&A	2024	2,700
Sontiq	M&A	2021	643
128 Technology	M&A	2020	448
CyberX (Network Management Software)	M&A	2020	170
suite3	M&A	2022	70
Threat Stack	M&A	2021	68
Kolide	M&A	2021	66
Noetic	M&A	2024	51
ZeroNorth	M&A	2020	40
Perception Point	M&A	2024	34