Bolstering Digital Defenses
Cybersecurity talent insights

Key Insights

- Cybersecurity Threats are on the rise - from 2016 to 2021, the number of cybercrime incidents in the United States has grown by 184% and monetary losses have grown by 360%, a total of $20.2bn USD based on FBI Reporting\(^1\). At this rate, the U.S. is projected to lose a total of $90.5 billion over the next 5 years, which is 0.39% of the U.S. GDP as of November 2022.

- Encouraging more community colleges to grant cybersecurity degrees will increase the pool of talent available to hire. Those with bachelor’s or higher qualifications in the U.S make up 88% of the cybersecurity workforce, -0.5pp since 2016). Legislation like the **National Community College Cybersecurity Challenge Act** can increase can also boost the supply of this talent.

- Pursuing skills-first hiring can offer significant gains by increasing the pool of talent available by up to 19X, according to LinkedIn data.\(^2\) The current active cybersecurity workforce represents 1.16% of the U.S. workforce, those with at least one cybersecurity skill or a relevant certification represent 6.7% (nearly 6 times more) of the workforce.

- Closing the gender gap in the cybersecurity workforce requires active intervention and would add 270,000 people to the talent pool. Women make up 19.1% (80.9% men) of the cybersecurity workforce globally and 18.7% in the U.S. This unbalanced gender ratio is worse than the technology industry where women make up 38% of the workforce (62% men).

---

\(^1\) Sources: FBI Internet Crime Report [2020, 2021]

\(^2\) Source: SkillsFirst: [Reimagining the Labor Market and Breaking Down Barriers, LinkedIn, 2023](https://www.linkedin.com/company/linkedin-economic-graph/)

**Akash Kaura**
Staff Data Scientist
Economic Graph
Research Institute
akash@linkedin.com

**Caroline Liongosari**
Data Scientist
Economic Graph
Research Institute
cliongosari@linkedin.com
Bolstering Digital Defenses

Cybersecurity threats are on the rise and security is a national priority

From 2016 to 2021, the number of cybercrime incidents in the U.S. has grown by 184% and losses have grown by 360%, a total of $20.2bn USD based on FBI Reporting.

Cybercrime Complaints and Losses (bn $)

Source: FBI Internet Crime Report 2020, 2021

The U.S. has been a frequent target of cybersecurity threats with 46% of observed activity targeted at organizations in the U.S. between July 2020 and June 2021 based on Microsoft data. The White House has made cybersecurity a key priority through various actions to bolster security including a focus on “building the Nation’s cyber workforce and strengthening cyber education.”

Nearly 1 in 43 (2.32%) jobs in the U.S. on LinkedIn are cybersecurity jobs (as of September 2022) increasing by 37% (CAGR) each year from 2016 to 2022. This pace was slightly slower than the

---

3 Microsoft Digital Defense Report, 2021
Bolstering Digital Defenses

39% (CAGR) for technology industry jobs which represent nearly 10% of all jobs on our platform in the U.S. (September, 2022). In 2021, 11% of hires were hired into cybersecurity jobs up from 9% in 2016. The bottom-line is that the frequency and complexity of attacks has been growing, and the demand for professionals to help organizations tackle them has been growing as well. Reflecting this demand and future growth prospects, the Bureau of Labor Statistics (BLS) puts the median salary of a cybersecurity analyst at $103k/year, making it the 3rd highest paid job category amongst their top 20 fastest growing occupations.

Supply of cyber talent is not growing fast enough

Surprisingly, against this backdrop of growing threats and competitive pay, organizations around the country are facing a shortage of skilled cybersecurity talent to hire. While the number of total cybercrime complaints has increased by 23% (CAGR) from 2016 to 2021, our data shows that the active cybersecurity workforce has only grown by 21% and continues to make up a small share of the total workforce in the U.S. (1.15% as of September 2021). The growth in job postings also outstrips the growth in the cybersecurity workforce by 17pp.

Growth in Cyber Incidents (complaints, losses), Workforce, and Job Postings

![Graph showing growth in cyber incidents, workforce, and job postings](source link)

*Source: LinkedIn Economic Graph*
Bolstering Digital Defenses

Utilizing the power of LinkedIn data, we have analyzed the dynamics of the cybersecurity workforce to surface some of the challenges and opportunities in developing a sustainable and diverse cybersecurity workforce.

Closing the gender gap in the cybersecurity workforce

We currently find that women make up 19.1% (80.9% men) of the cybersecurity workforce globally, which is an increase from 16.5% 5 years ago. In the U.S., this percentage is slightly lower with women currently making up 18.7% of the cybersecurity workforce. At the current rate, it would take 32 years to reach gender parity in the global cybersecurity workforce. This is slower than what it would take for the global cybersecurity workforce to reach gender parity (30 years) and the global technology workforce to reach gender parity (31 years). As such, there needs to be greater emphasis in presenting cybersecurity as a possible career choice for women as only about 0.5% of all women professionals work in cybersecurity. The share of male professionals in cybersecurity is nearly 4x this at 1.8%.

Encouraging women to choose cybersecurity as their career will take active efforts. This is especially true given that ratio of men vs. women is the Technology, Information and Media industry is 62/38 in favor of men, and that cybersecurity is even further from gender parity than technology. At LinkedIn, we have created our own initiatives to promote equity within the company and have published a report on the state of the workforce for women. There has also been a growth in non-profit organizations providing mentorship, training, and resources to encourage women to learn how to code and have careers in technology including Girls Who Code, Rewriting the Code, and AnitaB.org.

Such efforts will need to continue to bring more women into the cybersecurity workplace. If we reach gender parity based on the current number of men working in the field, we would be adding 270,000 people to the cybersecurity workforce that is in a significant need for talent.

Promoting skills-first hiring in cybersecurity

Our data also shows that the cybersecurity workforce is skewed towards those with Bachelor’s or higher qualifications in both the U.S. (88% of the cybersecurity workforce, -0.5pp since 2016), and globally (90.5%). STARs (Skilled Through Alternative Routes: members who have completed secondary education but do not have a bachelor’s degree nor have completed an apprenticeship program) on the other hand, only make up 11.5% of the cybersecurity workforce in the U.S. (up 0.5pp since 2016).
Bolstering Digital Defenses

Education Breakdown of the U.S. Active Cybersecurity Workforce (2022)

The share of cybersecurity jobs not requiring 4-year degrees has only increased by 40% between 2016 and 2022 compared to a 70% increase in the share of such jobs in technology, and 149% in the U.S. overall over the same period. This indicates that the barriers to entry for cybersecurity careers have been rising which does not bode well with businesses facing shortages when hiring skilled cybersecurity talent.

Jobs Not Requiring 4-Year Degrees

Source: LinkedIn Economic Graph
Bolstering Digital Defenses

It must be noted that jobs not requiring 4-year degrees are more prevalent in cybersecurity compared to technology overall indicating that organizations looking to hire cybersecurity talent are more amenable to skills-first hiring approaches compared to their technology industry counterparts. However, a clear challenge here is the lack of non-4-year cybersecurity degrees being awarded. In 2020, only 3,000 individuals graduated with an Associates degree in cybersecurity⁴. To address this, the National Community College Cybersecurity Challenge Act was introduced in September 2022 with the aim of expanding cybersecurity programs for community colleges⁵. In 2020, Microsoft also launched a national campaign to help community colleges expand the cybersecurity workforce⁶. In addition to increasing community colleges cybersecurity degree grants, partnerships with 4-year programs, and apprenticeships can also improve STARs career development prospects and serve as an effective response to the rising barriers to entry.

In addition to boosting the supply of community college graduates with cybersecurity degrees, certifications can also be an avenue to pursue skill-first hiring. LinkedIn data shows that nearly 2 in 5 cybersecurity job postings in the U.S. (1 in 3 globally) mention a cybersecurity related certification. In addition, as transitions into cybersecurity are becoming more frequent amongst U.S. members (going from 3.1% of all transitions in 2016 to 3.4% in 2021), the share of those who added a certification prior to doing so has also increased from 0.3% to 2.2% over the same period.

Cybersecurity Transitions and Certifications

---

⁴ Rep. McClain, Clarke Introduce Bipartisan National Community College Cybersecurity Challenge Act
⁵ H.R.8970 - National Community College Cybersecurity Challenge Act bill text
⁶ America faces a cybersecurity skills crisis: Microsoft launches national campaign to help community colleges expand the cybersecurity workforce – Brad Smith, President & Vice Chair, Microsoft
Bolstering Digital Defenses

Approaching hiring without the restraints of degree requirements and with a skills-first lens can also greatly expand the pool of available talent for organizations. Consider that while the current active cybersecurity workforce represents 1.16% of the U.S. workforce, those with at least one cybersecurity skill or a relevant certification represent 6.7% (nearly 6 times more) of the workforce. 12% of these professionals with cybersecurity skills or certification not currently holding cybersecurity jobs are in the technology industry. The top cyber security skills among these professionals include network, information, and cloud security, and vulnerability assessment. Hiring based on relevant skills can increase the talent pool by up to 19X in the U.S. (9.4X globally).

Conclusion

It is clear from the growth in cybercrime incidents and rise in monetary losses that cybersecurity is a significant threat in the U.S. and around the world. It is imperative that we take action in growing the cybersecurity workforce through multiple ways given the current shortage of cybersecurity professionals. First, by closing the gender gap within the cybersecurity workforce. This will be a major undertaking that will require outreach in many facets including providing mentorship to school-aged women via educational non-profit organizations such as Girls Who Code. In addition, companies and organizations looking to hire cybersecurity talent should create and grow initiatives to retain women. Such efforts have been enacted at LinkedIn for our own employees. Second, by pursuing skill-first hiring which requires providing alternative pathways towards a cybersecurity career other than 4-year college education such as community colleges and certifications. With these two major approaches in growing the cybersecurity workforce, we will work towards a safer future for everyone.
Bolstering Digital Defenses

Methodology

This analysis represents the world seen through the lens of LinkedIn data, drawn from the anonymized and aggregated profile information of LinkedIn’s 830+ million members around the world. As such, it is influenced by how members choose to use the platform, which can vary based on professional, social, and regional culture, as well as overall site availability and accessibility.

We have included data from 2016-September 2022 in this analysis. When referencing 2022, please take it to mean year-to-date unless otherwise stated.

The following countries are included in this analysis, and global analyses refer to aggregate data from all these countries combined:

- Argentina
- Australia
- Austria
- Belgium
- Brazil
- Canada
- Chile
- Colombia
- Costa Rica
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Iceland
- India
- Indonesia
- Ireland
- Israel
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Mexico
- Netherlands
- New Zealand
- Norway
- Peru
- Poland
- Portugal
- Romania
- Saudi Arabia
- Singapore
- Slovakia
- Slovenia
- South Africa
- Spain
- Sweden
- Switzerland
- Turkey
- United Arab Emirates
- United Kingdom
- United States

Members are considered ‘Cybersecurity Professionals’ if they hold one of the NICE aligned LinkedIn Occupations that we have identified as being Cybersecurity related. For more information on the crosswalk between LinkedIn Occupations and NICE Categories, please review our wiki. Further, if a member does not currently hold one of these selected occupations, and has >= 1 cybersecurity skill or certification completed, they are considered ‘Potential Cybersecurity Professionals’ for the purposes of this analysis.

Similarly, jobs are considered ‘Cybersecurity Jobs’ if the standardized occupation assigned to them is one of the selected occupations. Further, a job explicitly not requiring a 4-year degree is defined as a paid job containing the keywords like “no degree”, “GED”, “high school degree”, or “associate’s degree” in the job description.
Bolstering Digital Defenses

When referring to the technology industry, we refer to the combination of Technology, Information and Internet and Technology, Information and Media industries based on LinkedIn’s standardized industry taxonomy. More details on the taxonomy can be found here.

Within our member sample, we define three mutually exclusive member segments based on educational attainment:

- **STARs**: Members who have completed secondary education but do not have a bachelor’s degree nor have completed an apprenticeship program. This includes members who have an associate’s degree.
- **Apprenticeship**: Members who have completed an apprenticeship program but do not have a bachelor’s degree.
- **Bachelors**: Members who have completed a bachelor’s degree or higher. This may include members who have also completed an apprenticeship.

Cybersecurity courses and certifications were selected using text matching on course titles and certification provider name e.g., CompTIA, A+, Network+, CISSP, GIAC etc. Note that courses completed and certifications data are treated on a cumulative basis i.e., we count all members who have completed courses up to that point in time to calculate the cybersecurity shares.
Appendix