



VISA

Cybersecurity Talent in Demand

How Visa is Building the Payments
Workforce of the Future



Overview

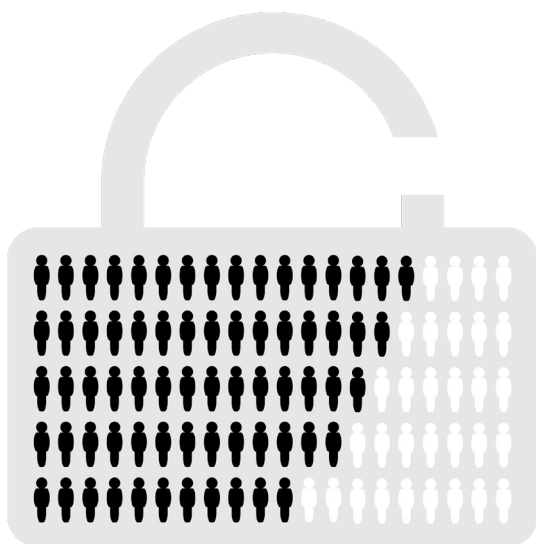
As the digital economy grows, so do cyber threats and our need for cybersecurity. In March 2023 alone, **41.9 million data records were compromised by cyberattacks** across the world—a **951% increase** since March 2022.¹ Over the next 12 months, **65% of organizations expect the number of cyberattacks to increase.**² With cyberattacks becoming more prevalent, cybersecurity has become increasingly critical as these threats become more complex, and ways to infiltrate networks become even more sophisticated.

This has created a demand for cybersecurity talent across all industries, but demand outpaces supply with global cybersecurity **job vacancies growing by 350%, with 3.5 million unfilled roles** in 2023.³ This paper will outline the challenges in not only the demand for cybersecurity talent, but what Visa is doing to address this issue as a workforce leader in the payments industry.

“We need not only enough people but the right people with the right skills in the right jobs to meet the growing cyber threat.”

—Andrew Garbarino (R-NY)⁴

House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection Chairman



In the US alone, there are **69 skilled cybersecurity workers for every 100 that employers need,**⁵ which puts both national security and the economy at risk as cyber threats increase. In an effort to address this growing need, on June 22nd 2023, the House Homeland Security Subcommittee on cybersecurity and infrastructure met to discuss this nationwide shortfall in cybersecurity talent. During this meeting, members of Congress, business leaders, and industry experts, came together to discuss the urgent need to close the talent gap in the cybersecurity workforce.

70%

of security leaders say they face **additional risks because of cybersecurity skills shortages**⁶

Why Now?

External market factors, disruptive payment trends, and a proliferation of digital ways to pay are all evolving the Payments Industry. New players like Big Tech⁷ and Fintechs⁸ are increasing their share of commerce by expanding payment offerings. Connected commerce is driving the digital economy and leading to new payments propositions, with a market size of \$240T.⁹

This evolution has set the stage for greater cybersecurity opportunities and threats. According to the World Economic Forum's Future of Jobs 2023 report, cybersecurity is one of the most strategically important skills for the workforce.¹⁰ It is estimated that by 2025, cyberattacks will cost the world over \$10T.¹¹ This has led to increased competition for cybersecurity talent. In a survey conducted by Fortinet Training Institute, **more than half (56%) of respondents indicate their organizations struggle to recruit cybersecurity talent.**¹²

Overcoming this shortage is critical for any organization, but it is particularly important in the Payments Industry to protect sensitive data, prevent potential losses, comply with regulations, and maintain customer trust.

New Payment Technologies Disrupting the Ecosystem

The introduction of payment technologies such as blockchain, cryptocurrencies and digital wallets are disrupting the traditional payments ecosystem. Along with this digital transformation, there is an increased reliance on digital infrastructure and greater access to computer processing power, enabling more ways for cyber attackers to break down systems and networks for fraudulent purposes. According to JP Morgan, 71% of organizations report having been victims of payments fraud attacks.¹³ As the number of digital payment transactions increase, payment companies not only need to enable faster, easier and more reliable transactions, but they must also ensure that the right security and protection for consumers and merchants is in place while meeting changing regulatory standards.

Having the right payments cybersecurity measures and the right talent in place with the right skills to monitor and mitigate payments cyberthreats is critical in establishing a secure payments ecosystem.

Diversity & Inclusion

Not only is it critical for companies to address the cybersecurity skills gap, but it is also important to look at increasing diversity, equity, and inclusion within this workforce. Historically, an over reliance on hiring talent with four-year college degrees resulted in limited access to hiring opportunities for marginalized groups. Now, the focus is moving from degree requirements to skills and experience. Apprenticeships provide critical skills training and development for those who don't have a technical four-year degree, democratizing access to opportunity.

A diverse and inclusive workplace helps attract top talent and also strengthens the overall workforce, cultivating a shared value system and better employee engagement. Research has shown that companies who have a more diverse and inclusive workforce are **1.7 times more innovative**.¹⁴ In fact, a McKinsey study found that **companies in the top quartile of ethnic and cultural diversity show 36% higher profitability than less-**

diverse companies.¹⁵ Therefore, increasing the diversity of cybersecurity talent is essential to help an organization identify risks and vulnerabilities and develop more effective security protocols.¹⁶

In a dynamic and ever-changing digital environment, diversity of perspectives, experiences, and backgrounds are necessary to broaden how cybersecurity teams think about, anticipate, and address cyber risks. According to a Diversity, Equity and Inclusion report from Aspen Digital Tech Policy Hub, only 4% of cybersecurity workers are Hispanic, 8% are Asian and 9% are Black.¹⁷ Less than 30% are women.¹⁸ These disparities mean that increasing the diversity of this workforce is critical to meeting cyber workforce demand and strengthening the ability for cyber teams to develop innovative solutions for future cyber risks. To address these challenges, companies must think differently about how they hire, develop, and retain the cybersecurity talent they need.



Addressing the Cyber Talent Shortage

Over the past five years, **Visa has invested more than \$9 billion on network security** to prevent cyber threats in the Payments Industry.¹⁹ Visa's real-time monitoring with AI has **blocked over \$4.2 billion in fraudulent payments** volume in 2022 and has deployed AI-enabled capabilities and always-on experts to protect their ecosystem, proactively detecting and preventing billions of dollars of attempted fraud.²⁰ More than a thousand dedicated diverse specialists have been employed to protect Visa's network from malware, zero-day attacks, and insider threats. As cyber threats increase in volume and sophistication, it is essential that Visa continues to grow their payments cybersecurity workforce.²¹

WHAT VISA IS DOING

Visa's position as a leader in consumer payments and an innovator driving emerging payment solutions means that Visa is well-positioned to take the lead on workforce development in critical areas such as payments cybersecurity, data and AI.



Investing in Employees

- Establishing a proactive approach to uplevel employee career journeys
- Offering specialized cyber training solutions



Building a Future Talent Pipeline

- Providing scalable training and certification programs
- Dedicated to developing a sustainable and diverse talent pipeline within the payments industry



Creating Attraction to the Payments Industry

- Educating local communities through partnerships with academic institutions and government organizations to upskill diverse talent populations

1

Investing in Employees

Visa Payments Learning Program will enable Visa to diversify pathways into tech/cybersecurity and offer industry-recognized learning courses and certifications to train and develop their internal and external workforce with necessary knowledge and skills.

One of the biggest opportunities for Visa to address the shortage of cybersecurity talent in the market is introducing upskill training programs to existing technology employees. According to a recent external talent trends report, employers like Visa are increasingly investing in talent strategies that focus more on professional development and growth.²² In an era of accelerated digital transformation, employees want to stay relevant through reskilling and upskilling initiatives provided by their employers. Companies are making more investments in learning and development, with 51% using upskilling and coaching as effective ways to address talent scarcity.²³ **Employees stay 41% longer at companies that regularly hire from within and three-quarters (73%) of employees say they would stay longer at their company if there were more skill-building opportunities.**²⁴

As part of the **Visa Payments Learning Program**, Visa is providing a development pathway for employees by providing them with courses that will result in Visa Payments Cybersecurity certification. These courses and certifications will not only benefit cybersecurity workers in their career path at Visa, but will enable them to validate their skills and help grow expertise in the industry. According to a recent study, 82% of company leaders indicated their tech employees would benefit from cybersecurity certifications. For example, 55% of employees indicated that cybersecurity certifications have sped up their career growth compared to 34% in 2021.²⁵ By empowering their talent to grow, Visa is providing employees with more opportunities, while addressing internal talent scarcity challenges and effectively filling critical roles.

2

Building a Future Talent Pipeline

When hiring for technical roles, employers would typically look for “traditional” candidates with a four-year degree in cybersecurity or related work experience. However, with the growing talent shortage, this recruiting approach must be expanded to consider new talent pools and diverse expertise to help organizations fill vacant positions.

In an effort to build a future talent pipeline for the payments industry, Visa is filling high-demand tech roles by launching alternative pathways into Visa. The **Visa Payments Learning Program** has a focus on developing talent with profiles outside of traditional four-year degrees. The program focuses on training multifaceted talent, such as those returning to the workforce, early-in-career, career changers, and military veterans by offering learning courses and certifications to bolster their knowledge base.

For example, **Visa’s Military Talent Program** actively recruits and hires military veterans, reservists, and military spouses and provides them with training and reskilling. By creating a pipeline of military-affiliated talent, Visa has an opportunity to provide training in areas such as payments cybersecurity that builds on their existing skillsets and rich diversity of experience.

Additionally, through **Visa’s Apprenticeship program**, Visa is attracting and training more diverse talent. Launched in 2023, an initial cohort of apprentices receive 16 weeks of specialist training, followed by a one-year apprenticeship. They are participating in Visa’s Payments Cybersecurity Introductory Course, with further intermediate and advanced courses and certifications to follow in 2024. 90% of the class identifies as diverse talent and receives on-the-job training, building technical and business skills needed to succeed as cyber professionals.

While this program is still in the process of scaling, apprentices in the first cohort have already excelled in the program— scoring 85% and above on their quizzes and assessments, with 100% of the apprentices rating the program as a great experience. Based on its success, Visa’s Apprenticeship program will be expanded in 2024 to additional cohorts.

3

Creating Attraction to the Payments Industry

As adoption of digital payment systems, contactless payments, and online transactions increase, the risk of fraud and data breaches also increase. To elevate awareness of these issues and attract new professionals with the critical cybersecurity skills, Visa is partnering with academic institutions, clients, and government organizations to grow the cybersecurity talent pool of the future.

More universities are implementing cybersecurity courses, and Visa plans to partner with educational institutions such as community colleges, technical schools and universities to offer 15-week semester courses, taught by trained and authorized college instructors to enrolled college students. Partnerships like these will provide students with training and career paths in cybersecurity and bring a pipeline of diverse, new talent. Community colleges in particular have a diverse student population—according to the American Association of Community Colleges, 30% of the nation’s community college students are the first in their families to attend college, with 39% identifying as Hispanic or Black and 5% being military veterans.²⁶ Partnering with these institutions will provide Visa and the broader payments industry with a talent pool to fill critical open jobs.

In addition, Visa will also offer its **Visa Payments Learning Program** to clients. This will enable clients to leverage cybersecurity best practices from Visa and grow their own cybersecurity talent, further helping to grow the number of payments cybersecurity experts in the industry. Launching in Q1 2024, Visa will offer virtual course offerings led by cyber team trainers.

Key Takeaways

Cybersecurity will continue to increase in importance as cyberattacks grow and skilled talent trained in payments cybersecurity will be critical to protect the payments ecosystem. The demand for cybersecurity talent is currently greater than the number of cyber workers in the market, and companies will have to close the supply-demand talent gap in creative, non-traditional ways.

Through the **Visa Payments Learning Program**, Visa is upskilling/reskilling employees, students, clients and military veterans through training and industry-recognized certification. Visa is taking the lead in the payments industry to not only ensure that it has the right skillset in place for its own employees, but also to further help safeguard the industry by creating a sustainable talent pipeline of cyber professionals from non-traditional and diverse backgrounds.

To learn more or enroll in the Visa Payments Learning Program, please visit:
www.VisaUniversity.com

1. Cyber Magazine: "41.9m records compromised by cyber breaches in March 2023," April 5, 2023, <https://cybermagazine.com/articles/41-9m-records-compromised-by-cyber-breaches-in-march-2023>
2. Fortinet: "2023 Cybersecurity Skills Gap Report," <https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf>
3. Cybersecurity Ventures: "2023 Cybersecurity Jobs Report," April 2023, <https://www.esentire.com/resources/library/2023-official-cybersecurity-jobs-report>
4. "House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection," June 22, 2023, <https://homeland.house.gov/2023/06/22/subcommittee-chair-garbarino-ro-bust-cybersecurity-workforce-is-needed-to-mitigate-risk-across-federal-networks-critical-infrastructure>
5. National Defense Magazine: "U.S. Desperately Needs Cyber Talent, Congress Says," June 26, 2023, <https://www.nationaldefensemagazine.org/articles/2023/6/26/us-desperately-needs-cyber-talent-congress-says>
6. World Economic Forum: "How reskilling and upskilling talent can help shrink the cybersecurity skills gap," April 26, 2023, <https://www.weforum.org/agenda/2023/04/how-reskilling-and-upskilling-talent-shrink-cybersecurity-skills-gap/>
7. "Big Tech" refers to the most dominant players in the tech industry such as Alphabet (Google), Amazon, Apple, Meta (Facebook), and Microsoft).
8. "Fintech" is a term used to describe "Financial technology" companies. These companies use technology to innovate, enhance, automate and digitize the design, delivery, and use of financial services for consumers and businesses.
9. Ernst & Young: "How the rise of PayTech is reshaping the payments landscape," https://www.ey.com/en_us/payments/how-the-rise-of-paytech-is-reshaping-the-payments-landscape
10. World Economic Forum: "The Future of Jobs Report 2023," April 30, 2023, <https://www.weforum.org/reports/the-future-of-jobs-report-2023/>
11. McKinsey: "New survey reveals \$2 trillion market opportunity for cybersecurity technology and service providers," <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers>
12. Fortinet: "2023 Cybersecurity Skills Gap Report," <https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf>
13. J.P. Morgan: "Staying Ahead of Payments Fraud and Cybersecurity Threats: Trends To Watch," <https://www.jpmorgan.com/content/dam/jpm/commercial-banking/insights/cybersecurity-infographic-afp-2022.pdf>
14. Fundera by Nerdwallet: "20 Diversity in the Workplace Statistics to Know," <https://www.fundera.com/resources/diversity-in-the-workplace-statistics#:~:text=Racially%20and%20ethnicall-ly%20diverse%20companies,are%201.7x%20more%20innovative.>
15. McKinsey & Company: "Diversity Wins: How Inclusion Matters," May 2020, <https://www.mckinsey.com/-/media/mckinsey/featured%20insights/diversity%20and%20inclusion/diversity%20wins%20how%20inclusion%20matters/diversity-wins-how-inclusion-matters-vf.pdf>
16. Forbes: "Minorities And The Cybersecurity Skills Gap," September 30, 2022, <https://www.forbes.com/sites/forbestechcouncil/2022/09/30/minorities-and-the-cybersecurity-skills-gap/?sh=1e5af3ff7f3f>
17. Aspen Tech Policy Hub: "Diversity, Equity and Inclusion in Cybersecurity," <https://www.aspentechpolicyhub.org/project/diversity-equity-and-inclusion-in-cybersecurity/>
18. Cybersecurity Ventures: "2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics," <https://cybersecurityventures.com/cybersecurity-almanac-2023/#:~:text=Cybersecurity%20Ventures%20expects%20global%20cybercrime,%243%20trillion%20USD%20in%202015.>
19. Visa: "New Visa Reports Underscore Importance of Cybersecurity Amid Shifting Threats," <https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.19166.html>
20. Visa: "New Visa Reports Underscore Importance of Cybersecurity Amid Shifting Threats," <https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.19166.html>
21. Visa: "Visa, a Technology Company - A Look at the technology behind global money movement" <https://usa.visa.com/dam/VCOM/global/about-visa/documents/visanet-factsheet.pdf>
22. Forbes: "Even During Uncertain Times, Companies Are Investing In People," March 1, 2023, <https://www.forbes.com/sites/rebeccahenderson/2023/03/01/even-during-uncertain-times-companies-are-investing-in-people-research-shows/?sh=7a2ec47e7562>
23. Randstad Enterprise: "2023 Global Talent Trends Report," <https://www.randstadsourceight.com/talent-trends/>
24. LinkedIn Talent Insights: "Employees Stay 41% Longer at Companies that Use This Strategy," March 4, 2020, <https://www.linkedin.com/business/talent/blog/talent-management/employees-stay-41-percent-longer-at-companies-that-do-this>
25. Fortinet: "2023 Cybersecurity Skills Gap Report," <https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf>
26. American Association of Community Colleges, "Fast Facts 2023," <https://www.aacc.nche.edu/research-trends/fast-facts/>