SISA

The Tipping Point:
Bridging the Cybersecurity Skill Gap in the Payments Industry Through Accredited Training

Table of Contents

The global payments renaissance amidst rising cyber threats

The global payments landscape is rapidly transforming, propelled by technology and evolving consumer demands. Traditional cash and check methods are giving way to a digital payments revolution, marked by the swift adoption of digital wallets, instant transactions, and innovative 'Buy Now, Pay Later' schemes. This evolution positions the payments industry at the dynamic crossroads of tech innovation, operational agility, and complex financial services.

> “In this dynamic, data is a bank's most valuable asset, constituting nearly 90% of a bank’s actionable customer insights.”

However, this upward trajectory of global payments casts a shadow — the dark underbelly and mounting risk of cybersecurity threats. The payments sector stands vulnerable, more than ever, to a myriad of increasingly sophisticated threats, especially those targeting payment card data. SISA’s research reveals a concerning trend: In 2022 alone, the payments sector witnessed 400 breaches, which constituted a significant 10% of the total reported data breaches. Underlining the gravity of the situation, IBM’s Cost of a Data Breach Report 2023[1] indicates that the financial sector endures the second-highest average cost per breach, just behind healthcare. These breaches are particularly costly, with financial organizations averaging **$5.97 million** in damages per incident, 28% higher than the global average[2].

> “Recent survey indicates that 81% of bankers expect to see a spike in cyber threats with 43% stating that their bank is ill prepared to protect customer data, privacy and assets in the event of an attack[3].”

Fraudsters are showing remarkable adaptability, constantly innovating around digital payment systems. With the advent of Real Time Payments (RTP), we are seeing a proliferation of new fraud types—from traditional threats like phishing and malware to emerging fraud mechanisms involving fake payment links, OTP manipulations, social engineering schemes, spoofing attacks - the cybersecurity landscape is as dynamic as it is menacing. The sector is further navigating an increasingly intricate labyrinth of regulations, with data protection norms and privacy standards in constant flux.

To guard against these multifaceted threats, it's imperative for organizations to cultivate a well-trained and dedicated workforce. And herein lies the dichotomy. This talent, as crucial as it is, finds itself in stark deficit, undermining the integrity of the digital-dependent financial infrastructure.

According to Fortinet’s 2022 Cybersecurity Skills Gap Report[4], 80% of organizations suffered one or more breaches that they could attribute to a lack of cybersecurity skills and/or awareness. The shortage of qualified personnel significantly impairs the payment organization's ability to fend off and respond to cyberattacks, thereby making data breaches not just possible, but increasingly likely.

A brewing crisis: The escalating cost of the cybersecurity skill gap

The cybersecurity skill gap isn't breaking news; it's a pressing headline that just won't go away. The Carnegie Endowment for International Peace isn't mincing words when it identifies this talent crisis as one of six critical priorities for fortifying financial systems against cyber onslaughts. A recent industry survey reveals that more than 50% of organizations report insufficient cybersecurity staffing that puts them at 'moderate' to 'extreme' risk of a cyber-attack[5].

Quantifying the cyber talent gap in payments: A SISA perspective

Cybersecurity gap in payments industry

Global cyberattack damages escalating

Financial impact on payments and financial services

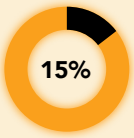
Current deficit

Approximately 350,000 professionals needed

For every 875 unfilled roles, the risk of a data breach escalates

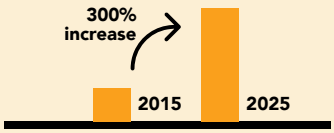
Risk amplification

Projected growth



Rise in annual damages, globally

Staggering costs



Estimated to reach **$10.5 trillion** by 2025, a **300% increase** since 2015.

Sector-specific forecast

Anticipated costs for the sector may soar to $2.3 billion.

> "The current shortfall of professionals is akin to navigating the treacherous waters of digital payments with undermanned teams, much like sailing through a storm with half a crew."

Projected fallout beyond breaches

Executive Viewpoint by
Dr. Rajan R, VP, SISA Institute

The cybersecurity skills gap is a well-documented concern, often highlighted in the context of breaches and direct attacks. However, the undercurrents of this deficit run deeper, leading to repercussions that could potentially impact customer trust, damage reputation and disrupt operations of the payments business.

The payment industry is no stranger to stringent compliance requirements. With global regulatory bodies ratcheting up cybersecurity stipulations, organizations are finding themselves in a perpetual race against ever-stringent standards. A prime example of this is the mandated annual security assessments required by the Payment Card Industry Data Security Standard (PCI DSS). The dearth of qualified QSAs (Qualified Security Assessors) has transformed what should be a routine procedure into a compliance bottleneck, leading to delays, fines, and in some cases, severe penalties for non-compliance. Yet, this is but the tip of the iceberg. The skills shortage extends its tendrils into the day-to-day operations, affecting the ability of payment organizations to effectively monitor for threats. Cybercriminals are becoming increasingly sophisticated, employing advanced techniques like generative AI and Large Language Models (LLMs) to orchestrate attacks. In addition, the volume of data being processed by payment systems is increasing, which makes it more difficult to monitor for threats, and consequently making it more lucrative for bad actors to exploit them using novel tactics. The widening skills gap is more than just numbers; it manifests as misconfigured systems, tardy patching of systems, inadequate oversight, and hasty deployments creating fertile ground for more potent cyberattacks.

Furthermore, this shortfall strikes at the heart of innovation. In an industry that thrives on the cutting edge, the lack of robust cybersecurity expertise is a significant impediment. It's not merely about crafting new solutions, but ensuring these innovations are robustly secure. The prevailing cybersecurity skills gap is a substantial roadblock, often meaning organizations lack the expertise to safely harness and embed new technologies. This duality—of needing to innovate but being stymied by the lack of agile cybersecurity skills—creates a precarious balancing act. Firms frequently find themselves diverting essential resources from pioneering projects to mitigate immediate cyber threats.

The web of interconnectivity in the financial ecosystem amplifies these risks, with third-party vendors and suppliers representing a multitude of additional vulnerability points.

In my perspective, addressing this skill gap is not just a matter of hiring more professionals; it is about creating a sustainable ecosystem of continuous learning and adaptation. We must foster a culture where cybersecurity is not the sole domain of specialists but an integrated discipline within the fabric of every role in the payment industry. As daunting as the challenge may seem, it presents us with an opportunity to reimagine our approach to cybersecurity training, talent development, and operational resilience. The future of payment security, after all, hinges on our ability to do so.

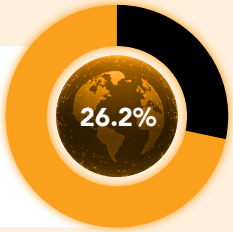
Pieces of the puzzle: What's fueling the skill shortage?

Talent deficit

43%

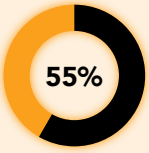
Companies identify a lack of qualified cybersecurity talent.

Global workforce gap widened by 26.2%, now at 3.4 million[6].



Essential to invest in training, retention, and employee growth.

Training void

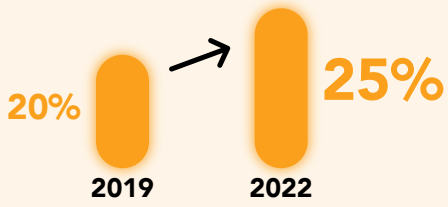


Banking execs focus on training current staff vs. hiring new[7].

Continuous training is critical, yet implementation lags.

Talent gap uncovered

Diversity drought



Women constitute only 25% of the cybersecurity workforce in 2022, up from 20% in 2019[8].

Diversity fosters innovative solutions and is crucial for tactical threat understanding.

Agility absence

Cybersecurity roles require an agile skillset to match rapid threat evolution.

Static education models lead to outdated and ineffective defenses.

Novel attacks, like the Beanstalk Farms heist, highlight the need for updated skills[9].

Harnessing certification to bridge the talent divide

Wearing the Badge of Honour - The Crucial Role of Accredited Cybersecurity Education

With payments industry battling a growing cybersecurity skills shortage, it is crucial to equip individuals with the skills required to tackle real-world cyber threats. Closing the skills gap will require a two-pronged strategy that involves:

Training and educating more individuals in skills that are in high demand

Creating policies and programs that support the ongoing learning & development of cybersecurity professionals.

Specialized certifications play a critical role and are increasingly being sought after by organizations as proof of industry knowledge and skills. According to Fortinet's 2023 Cybersecurity Skills Gap Report[10], 82% of respondents indicate their organization would benefit from cybersecurity certifications, and 90% indicate they would pay for an employee to obtain a cybersecurity certification.

Specialized, accredited cybersecurity education programs impart hands-on experience, ethical hacking skills, and an understanding of legal/regulatory implications. Industry-recognized certifications, such as SISA's ANAB-accredited payment industry security certifications are key to create a sustainable pipeline of skilled cybersecurity professionals. These certifications provide an assured benchmark for employers, boosting their confidence in hiring decisions. Furthermore, SISA's own learnings from global forensic investigations have shown that organizations with certified cybersecurity professionals are more resilient to cyberattacks. Some of the major benefits of globally accredited payments industry certifications are:

They serve as industry markers to validate individual skills, lending credibility and confidence for employers looking to hire new talent.

They aim to establish not only technical competencies but also a deeper understanding of how to apply those competencies in a dynamic and evolving payment landscape.

They provide individuals a robust and recognized pathway to advancement within the field of payment Industry.

They lead to positive business results through higher retention and better performance by employees.

To bridge the skills gap, fostering a learning-centric work environment is key. Collaborations between industry, academia, and regulatory bodies, along with diversified hiring practices, including women, minorities, and veterans, are essential to enrich the talent pool and promote workforce development.

SISA - Stronger together: Fostering collaboration for talent nurturing

SISA Institute (SISA's cybersecurity training arm), a pioneer in ANAB-accredited payment industry security certifications has been at the forefront of tackling this challenge, through providing top-notch education and training for payment Industry security professionals. Being the first Payment Data Security Certification in the world to achieve accreditation by ANAB, a global accreditation body with a rich legacy of promoting standardization and conformity assessment, SISA Institute's payment certifications adhere to the stringent requirements, internationally recognized standards and best practices established by ANSI. With 15+ years of proven track record of training and certifying over 10,500 professionals from over 2,000+ customers spread across 40 countries, SISA's certifications are widely recognized for high quality of instructors and the unique forensics-driven approach to cybersecurity.

SISA's CPISI, CPISI-Advanced and CPISI-Developers ANAB-accredited certification programs are designed to address the demanding requirement of payment data security professionals for the digital payments age encompassing all form factors of payments and covering relevant standards, regulations, and best practices. These certifications enable payment organizations to hire and elevate professionals who demonstrate this expertise with internationally accredited certifications. SISA's training programs are suitable for individuals who are responsible for implementing and maintaining security controls within organizations that handle payment data. This may include IT professionals, security analysts, compliance officers, and individuals involved in managing the compliance to regulatory standards.

The advantages of taking SISA's certifications are multifold:

Hybrid mode of training that offers flexible learning options through self-paced videos and weekly live instructor-led sessions

Integration of practitioner insights and forensic learnings to improve security controls with real-world lessons and applications

Continuous learning opportunities through access to webinars, research, content assets and Forensic Learning Sessions (FLS)

Membership to a growing community of passionate learners and industry experts for networking and professional growth

To conclude, SISA's payment security certifications offer a competitive edge to candidates looking to build a career in cybersecurity. While for organizations, they help to comply with industry regulations or security standards, in addition to serving a qualified pool of talent, ready to tackle the dynamic threat landscape and making them future-ready.

Closing thoughts

In closing, the cybersecurity skill gap presents a significant and multifaceted challenge to the payment industry—a sector where the stakes of digital security are perpetually high and ever-increasing. The deficit in skilled professionals does more than expose businesses to potential breaches; it undermines the ability to comply with rigorous regulations, it stifles the innovation essential for competitive advantage, and it weakens the ecosystem's overall capacity to pre-empt and resist the sophistications of cyber threats.

The solution to this pervasive problem is not merely in increasing headcounts but in elevating the expertise of each professional within the industry. Cybersecurity certifications are crucial in this endeavor. They represent a commitment to the continuous advancement of skills, to the embodiment of best practices, and to the proactive defense of our critical payment infrastructures.

Prioritizing these certifications is an essential strategy for businesses seeking to fortify their defenses and ensure a secure transactional environment for their customers. It is through this lens that organizations must view their talent development programs—not as a regulatory checkbox, but as a foundational element of their cybersecurity strategy.

> “As we stand at this juncture where payment systems are increasingly interconnected and data flows are becoming more complex, the call to action is clear. Embracing certifications is a step that cannot be deferred, for the security of our data, the trust of our customers, and the integrity of the payments industry depend on our willingness to act and invest in the cybersecurity professionals of today and tomorrow”

Dharshan Shanthamurthy,
Founder & CEO at SISA

References

1. IBM Cost of a Data Breach Report, 2023
2. Security Intelligence - Cost of data breach 2023
3. KPMG 2023 State of Banking Industry Survey
4. Fortinet Cybersecurity Skills Gap Report 2022
5. ISC2 Cybersecurity Workforce Study, October 2022
6. ISC2 Cybersecurity Workforce Study 2022
7. Only 55% bank execs prioritize cybersecurity training for staff, American Banker, August 2022
8. Women hold 25% of cybersecurity jobs in 2022, Cybersecurity Ventures report
9. Beanstalk loses $182 million in crypto heist, The Guardian, April 2022
10. Fortinet 2023 Cybersecurity Skills Gap Report

Key Authors

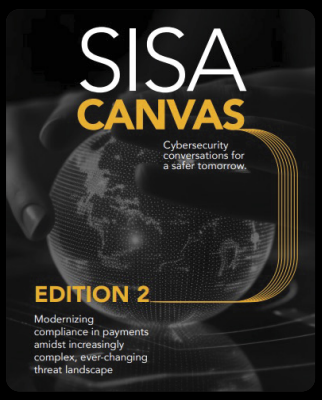
Dr. Rajan R - VP, SISA Institute, SISA

Aparna Gajanan - Sr. Director, Brand and Communications, SISA

Radhika Kamath - Sr Content Lead, SISA

Access our knowledge assets on all things cybersecurity!

Thought leadership to build cyber resilience.



Scan to discover how we shield customers!

Forensics cybersecurity triumphs with our clients.

Boosting payment security: ProACT MDR elevates threat detection & response!

Achieving PCI DSS compliance in Egypt & Qatar.

SISA's Red Team: revealing & reinforcing co-op bank defenses!

Scan for insights!

Latest round-up on threats and exploits.

DDoS attacks on IoT devices skyrocket in 2023.

Fake telegram apps infect 10 million users with spyware.

New superbear trojan emerges in targeted phishing attacks.

Scan for top threat summaries!

About SISA

SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective cybersecurity solutions. Our problem-first, human-centric approach helps businesses strengthen their cybersecurity posture. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

SISA is one of the leading global forensic investigators for the payments industry.

1,000+
Active engagements

2,000+
Global customers served

40+
Countries

Global Presence

USA | Canada | UK | Bahrain | Saudi Arabia | UAE | Qatar | India | Singapore | Malaysia | Australia