

Cybersecurity in Emerging Markets



Table of Contents

1.0 Introduction	
1.1 Executive Summary	05
2.0 Cybersecurity in the Banking Industry	
2.1 Evolving Landscape of Cyber Threats	07
2.2 Recent Cyber-Attacks and Their Impact	10
2.3 Financial Institutions' Spending on Cybersecurity	12
2.4 Key Insight and Analysis	15
2.5 What are the Industry Experts Saying?	16
3.0 Cybersecurity Landscape in Emerging Markets	
3.1 Industry Share of Cyber-Attacks	18
3.2 Cybersecurity Readiness in Emerging Markets	20
3.3 Cybersecurity Measures Implemented in Emerging Markets	23
3.4 Technological Frontiers in Cybersecurity Space	26
3.5 Solutions within the Cybersecurity Domain	27
3.6 What are the Industry Experts Saying	31
4.0 Key Takeaways and Future Outlook	32





Introduction



Cybersecurity in banking refers to the **set of measures, technologies, practices, and policies implemented by financial institutions to protect their computer systems, networks, and data from unauthorised access, cyberattacks, and other forms of digital threats**. The primary goal of cybersecurity in banking is to safeguard sensitive financial information, maintain the integrity of banking operations, and ensure the confidentiality of customer data.

According to Allied Market Research¹, the global market for cybersecurity in banking, valued at \$74.3 billion in 2022, is anticipated to reach \$282 billion by 2032, exhibiting a robust compound annual growth rate (CAGR) of 14.4% from 2023 to 2032. This sector addresses the technologies and procedures designed to prevent and counteract cyberattacks targeting the data, networks, and digital infrastructure of financial institutions. The allure of the financial sector to hackers is evident due to its wealth of sensitive data and financial assets. The industry faces significant challenges, including potential vulnerabilities associated with remote work and risky customer behaviours such as password sharing during digital banking, which can be challenging to mitigate.

The surge in the cybersecurity in banking market is closely tied to the ongoing digital transformation within the banking sector. Many banks and financial institutions are adopting an omni-channel approach to enhance the overall customer experience. The integration of digital banking services allows these entities to simplify and streamline banking processes, making them more accessible and convenient for a global population.



Executive Summary

The cybersecurity landscape has witnessed profound shifts, notably in the banking sector, with a spotlight on emerging markets. According to CB Insights (see Fig. 2.2) , the finance and insurance industry in 2022 faced persistent cyber threats, constituting 18.9% of attacks, driven by evolving techniques like zero-day exploits, malware, and social engineering. Data breaches, fuelled by financial gain, remained prevalent, prompting industries to fortify digital defences amidst the complex and interconnected cybersecurity landscape exacerbated by the COVID-19 pandemic.

Simultaneously, emerging market banks are escalating cybersecurity spending in response to the evolving threat landscape. With a promising outlook, technological advancements such as AI, IoT, Blockchain, and 5G drive this surge, as evidenced by a robust 16% CAGR in cybersecurity investments from 2014 to 2018, accelerating in subsequent years. This reflects a strategic commitment within the BFSI sector to leverage digital technologies for enhanced operational efficiency and superior customer experiences.

Regional cybersecurity readiness exhibits disparities, with Saudi Arabia and the UAE leading in the MENA region, Brazil standing out in South America, and Singapore excelling in Southeast Asia. However, challenges persist, emphasising the need for cohesive regional strategies and collaboration, particularly in countries like Argentina, Indonesia, and the Philippines, where performance gaps indicate an urgency for collective measures.

Technological advancements, particularly AI and machine learning, play a pivotal role in shaping cyber risk strategies, with 20% of respondents recognising their influence. Cloud technology closely follows at 19%, highlighting a holistic approach to technology adoption. Meanwhile, Q3 2023 witnesses a 12% increase in venture funding for cybersecurity startups, reaching almost \$1.9 billion, but a notable 30% decline from Q3 2022 signifies a nuanced funding landscape. This dynamic scenario underscores the sector's resilience, adaptability, and reliance on cutting-edge technologies to combat evolving cyber threats. The ongoing narrative of the cybersecurity journey necessitates collaboration between industry leaders, innovative startups, and policymakers to fortify our digital future against emerging challenges.





Cybersecurity in the Banking Industry

Evolving Landscape of Cyber Threats

Amid digital transformation and fintech innovations, the banking sector in emerging markets grapples with an increasingly sophisticated and dynamic landscape of cyber threats, making it an attractive target for cybercriminals pursuing financial gain or broader geopolitical objectives.

In the realm of cyber threats in banking, traditional cybercrime methods like ransomware and phishing attacks have undergone refinement, incorporating advanced techniques that pose a serious risk to financial data. A particularly noteworthy technique, as revealed by the McAfee Threats Report,¹ is the use of zero-day exploits, which target undisclosed vulnerabilities in software or hardware, exploiting the lack of a patch (no software updates or fixes) and making them potent tools for cybercriminals.

Malware, a common element in these sophisticated cyber-attacks, plays a pivotal role in compromising the security of banking systems. Malicious software, or malware, encompasses a range of harmful programs designed to infiltrate, damage, or gain unauthorised access to computer systems. In the context of the banking sector, malware may be deployed to steal sensitive financial information, compromise the integrity of transactions, or enable unauthorised access to networks.

Furthermore, the interconnected nature of the global financial ecosystem has presented new challenges, with cyber attackers strategically targeting the supply chains of banks. This involves compromising third-party vendors to gain unauthorised access to banking networks, a tactic emphasised in the Accenture State of Cybersecurity Report.²

¹ McAfee. (2023). What is a Zero-Day Threat? Retrieved Nov 2023, from <https://www.mcafee.com/learn/what-is-a-zero-day-threat/>

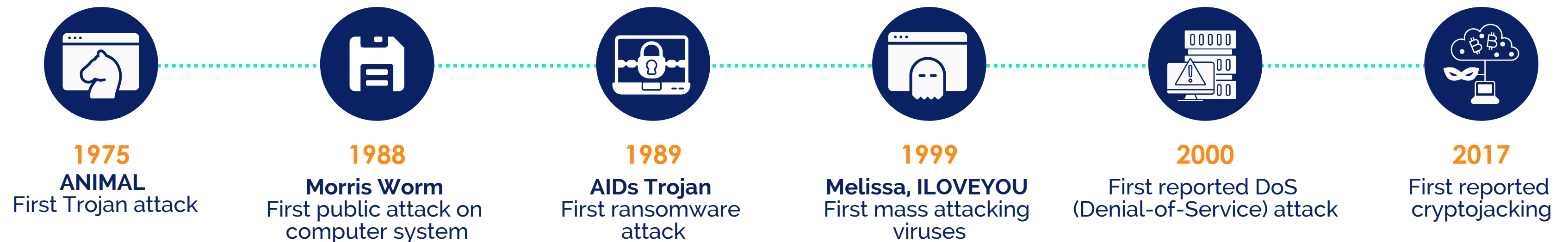
² Accenture. (2023). Aligning Cybersecurity to Business Objectives Helps Drive Revenue Growth and Lower Costs of Breaches, Accenture Report Finds. Retrieved June 2023, from <https://newsroom.accenture.com/news/2023/aligning-cybersecurity-to-business-objectives-helps-drive-revenue-growth-and-lower-costs-of-breaches-accenture-report-finds>



In parallel, the rise of mobile banking, while enhancing convenience, introduces a distinct avenue for cyber threats. Malware specifically tailored for mobiles, may target banking apps or exploit vulnerabilities in mobile operating systems, compromising the security of financial transactions and sensitive customer data. The Verizon Mobile Security Index¹ documents instances of vulnerabilities associated with smartphones, which may in turn affect mobile banking experience, underlining the urgency for financial institutions to fortify their mobile security infrastructure. According to the report, nearly 27.5% of the phishing links sent to enterprise devices and 54.2% of the phishing links sent to personal devices have been clicked. Despite this, nearly two-thirds (65%) of companies still do not perform phishing simulations.

Social engineering, another facet of the evolving cyber threat landscape, adds a human element to these attacks. This technique involves manipulating individuals into divulging sensitive information or performing actions that compromise security. In the context of banking, social engineering attacks might involve impersonating legitimate entities to trick employees into providing access credentials or convincing customers to disclose personal information. This user-focused approach highlights the need for not only technological safeguards but also robust education and awareness programs within financial institutions to mitigate the risk of social engineering attacks.

The following timeline shows the evolution of cyber threats:



Evolution of Cyber Threats



1975

ANIMAL - First Trojan attack

ANIMAL, a Trojan virus, was released in 1975. Trojan viruses are malicious programs that disguise themselves as legitimate programs. Once installed on a computer, a Trojan virus can steal data, install other malware, or disrupt the computer's operation.



1988

Morris Worm - First public attack on computer system

Morris Worm, which was released in 1988, was the first major worm to be released on the internet. Worms are self-replicating programs that can spread rapidly from computer to computer. The Morris Worm caused widespread damage to computer systems around the world.



1989

AIDs Trojan - First ransomware attack

In 1989, the AIDs Trojan was released. This was the first ransomware attack. Ransomware is a type of malware that encrypts a victim's data and demands a ransom payment in exchange for the decryption key.



1999

Melissa, ILOVEYOU - First mass attacking viruses

Melissa, ILOVEYOU, which was released in 1999, was the first major mass attacking virus to be released on the internet. These viruses are self-replicating programs that can spread rapidly from computer to computer. The Melissa and ILOVEYOU viruses caused widespread damage to computer systems around the world.



2000

First reported DoS (Denial-of-Service) attack

In 2000, the first denial-of-service (DoS) attack was reported. DoS attacks are designed to overwhelm a computer system or network with traffic, making it unavailable to legitimate users.



2017

First reported cryptojacking

In 2017, the first cryptojacking attack was reported. Cryptojacking is a type of malware that uses a victim's computer to mine cryptocurrency. Cryptocurrency mining is a computationally expensive process, and cryptojacking can significantly impact the performance of a victim's computer.

FIGURE 2.1

Recent Cyber-Attacks and Their Impact

Over the years, cyber attacks on financial institutions have exhibited discernible patterns, revealing the evolving landscape of threats faced by various entities from 2007 to 2022 as recorded by Carnegie Endowment.

Data breaches stand out as the most prevalent form of attack, with 11 out of 13 incidents involving the unauthorised extraction of data from financial institutions. These breaches compromised a spectrum of sensitive information, including customer account details, credit card numbers, and Social Security numbers. Financial institutions of varying sizes, from multinational banks to smaller prepaid card companies, have become targets.

Cyber attackers are employing progressively sophisticated methods, making their activities harder to detect. For instance, the 2018 JPMorgan Chase data breach involved a combination of social engineering and malware, showcasing the evolving tactics used by attackers to infiltrate financial institutions. A notable trend is the targeting of cryptocurrency exchanges, evident in the 2019 Zaif Crypto Heist and the 2021 Bitmart security breach. This shift suggests that cybercriminals are adapting to new opportunities presented by the rise of cryptocurrencies.

The motivations behind these cyber-attacks are diverse, but financial gain remains the predominant driver. Stolen customer data is often monetised on the dark web or used directly for fraudulent activities. Additionally, some attacks have espionage purposes, highlighting the multifaceted motivations within the cyber threat landscape.

Take a look at some of the biggest cyber-attacks year-on-year from 2007 to 2023:



Timeline of the Biggest Cyber-Attacks



FIGURE 2.2
TIMELINE OF THE BIGGEST CYBER-ATTACKS

Financial Institutions' Spending on Cybersecurity

Cybersecurity spending by banks in emerging markets is on the rise, driven by a number of factors, including the increasing sophistication of cyberattacks, the growing adoption of digital banking services, and the increasing regulatory scrutiny of cybersecurity risks.

The period from 2014 to 2018 witnessed a transformative synergy between traditional financial institutions and the burgeoning realm of cybersecurity startups. Two critical facets of this evolution are discernible through the lens of banks' direct investments in cybersecurity and the parallel surge in venture capital funding for cybersecurity startups.

On one front, established banks recognised the imperative to fortify their own digital perimeters. According to CB Insights¹, the total amount of cybersecurity investment by banks in emerging markets increased from \$174 million in 2014 to \$349 million in 2018. This represents a compound annual growth rate (CAGR) of 16%. These investments ranged from threat intelligence to data security. Notably, a report by Global Data² stated that the retail banking sector generated \$7.9 billion in global cybersecurity revenue in the year 2020. They also predicted the industry to grow at 8% CAGR till 2025.

Simultaneously, the years from 2014 to 2018 witnessed a 55% surge in funding for innovative startups dedicated to addressing the evolving landscape of cyber threats, according to Statista³. These startups, nimble and innovative, brought fresh perspectives and cutting-edge solutions to the cybersecurity domain. VC funding not only provided the necessary capital for these startups but also nurtured an environment conducive to experimentation and disruptive thinking.



Investments and Fundings in Cybersecurity



FIGURE 2.3
BANK INVESTMENTS IN CYBERSECURITY

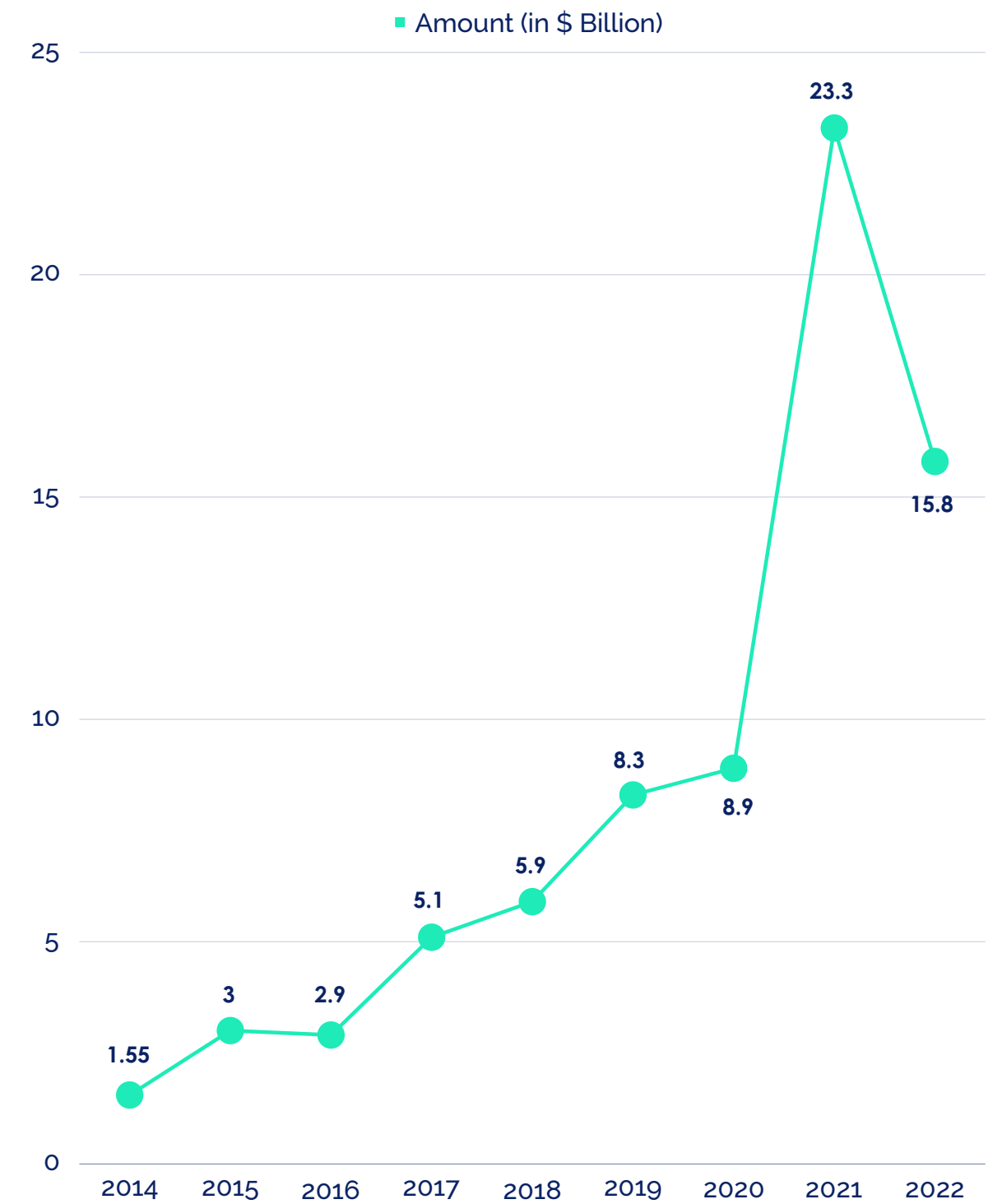


FIGURE 2.4
VC FUNDING IN CYBERSECURITY



Technological Advancements Affecting Cybersecurity



**Artificial Intelligence
(AI)**



**Internet of Things
(IoT)**



Blockchain



5G

The cybersecurity in banking market is thriving due to technological advancements like AI, IoT, Blockchain, and 5G, with IoT and AI reshaping traditional processes in the BFSI sector. Banks, facing regulatory pressures, are adopting innovative approaches to enhance efficiency and customer experiences.

BFSI companies are leveraging digital tech to revolutionise payments and streamline KYC processes, integrating IoT and AI to transform backend operations and establish a robust financial infrastructure, enabling automated payments through sensors, tracking devices, NFC chips, and applications.

Key Insight and Analysis

Cybersecurity spending in emerging market banks is rising due to the evolving threat landscape, with a promising outlook driven by technological advancements like AI, IoT, Blockchain, and 5G, as the BFSI sector integrates digital technologies to enhance operational efficiency and customer experiences. The investments by banks on cybersecurity were going at a 16% CAGR from 2014 to 2018 and has only accelerated since then.

Cyber threats have evolved significantly from 1975 to 2023, with an increasing focus on the banking sector, especially in emerging markets. In 2022, the finance and insurance industry accounted for 18.9% of cyber-attacks, reflecting the persistent targeting of financial institutions. The evolution includes sophisticated techniques like zero-day exploits, malware, and social engineering, posing serious risks to financial data. Data breaches, driven by financial gain, remain prevalent, affecting entities across the financial spectrum. The COVID-19 pandemic further heightened vulnerabilities, necessitating industries to fortify digital defences in an interconnected and rapidly evolving cybersecurity landscape.



What are the Industry Leaders Saying?



A robust cybersecurity culture is a must for banks as data breaches and cyber incidents are very uncertain in the growing technology space. It may cause severe complications for banks if they are non-compliant or vulnerable to their existing security posture as its important in today's threat landscape.

Kavitha Srinivasulu¹

Global Head, Cyber Risk & Data Privacy R&C BFSI





Cybersecurity Landscape in Emerging Markets

Industry Share of Cyber-Attacks

As our world becomes increasingly digitised, the spectre of cyber threats looms larger than ever, posing significant challenges across industries. Among these, **the manufacturing sector has consistently found itself in the crosshairs of cyber-attacks, accounting for nearly a quarter of all incidents in 2020, 2021, and 2022.** This persistent targeting reflects the allure of manufacturing companies to cybercriminals, given the treasure trove of valuable data they harbour, including intellectual property, production schedules, and customer information. In the cybersecurity landscape of 2022, finance and insurance emerged as the second most targeted industry, representing 18.9% of cyber-attacks. Financial institutions, holding vast reserves of sensitive customer data such as credit card numbers and bank account information, make for lucrative targets.

Beyond these industry-specific trends, **the cybersecurity realm experienced seismic shifts catalysed by the COVID-19 pandemic.** The rapid transition to remote work environments heightened vulnerabilities, exposing businesses to increased risks of cyber-attacks. Moreover, the surge in the use of remote access tools, necessitated by the pandemic, became a focal point for cybercriminal exploitation as they sought unauthorised entry into corporate networks.

In this dynamic landscape, understanding the nuances of cyber threats becomes imperative. The following insights delve into the specific data reflecting cyber-attack patterns across industries in recent years, shedding light on the evolving strategies of cyber adversaries and the industries that must be especially vigilant in fortifying their digital defences.



Industry Share of Cyber-Attacks

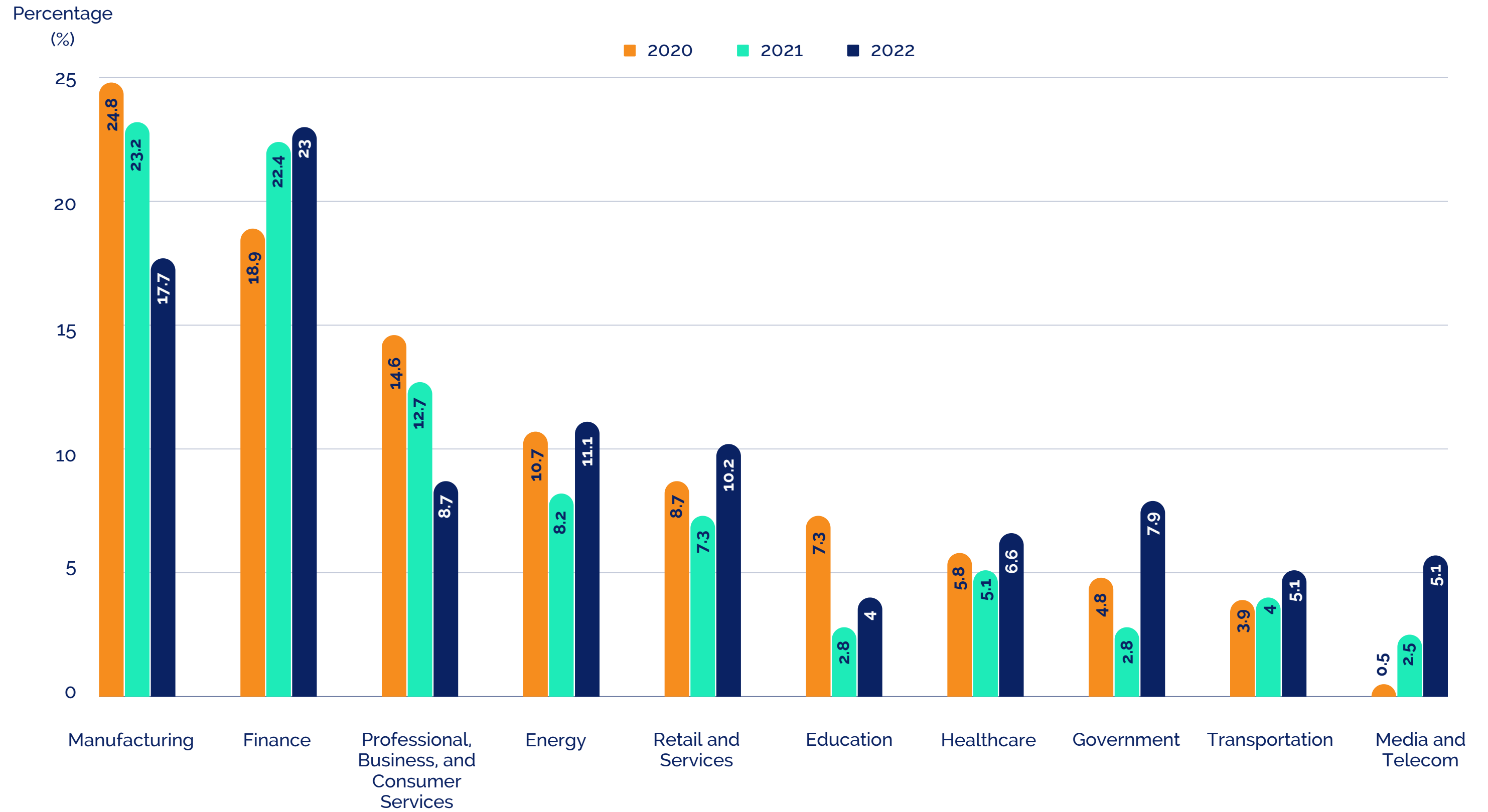


FIGURE 3.1

Cybersecurity Readiness in Emerging Markets

Countries in the Middle East are rapidly embracing digitisation, characterised by the widespread adoption of connected digital technologies and applications across consumers, businesses, and governments. According to a UBS report,¹ **the digital economy in the Middle East is anticipated to expand over fourfold, reaching approximately \$780 billion by 2030.** This growth is set to outpace the global average, with the digital economy expected to surge from an estimated \$180 billion in 2022. The projected compound annual growth rate for the digital economy in the region is more than 20%, signalling a transformative trajectory throughout the coming decade. In alignment with this perspective, a study conducted by ASEAN.org² suggests that the ASEAN digital economy framework holds the capacity to twofold the region's digital economy, elevating it from \$1 trillion to \$2 trillion by the year 2030.

The Middle East and North Africa (MENA), Southeast Asia (SEA) and some of the South American regions, with their abundant resources and rapid adoption of digitisation, have become enticing targets for a diverse range of cyber threats. Governments and major organisations across various vital sectors in the region have experienced damage from cyber-attacks. It is noteworthy that these regions are not passive recipients of cyber threats; rather, they are proactively taking measures to address these challenges. The International Telecommunication Union (ITU) has recognised their efforts, leading to commendable global and regional rankings based on their commitment to cybersecurity and proactive actions against cyber threats.

The Global Cybersecurity Index (GCI) 2020, compiled by the International Telecommunication Union (ITU), offers a comprehensive view of cybersecurity readiness worldwide. In this section, we delve into both the global and regional performances of the Middle East and North Africa (MENA), South America, and Southeast Asian countries, exploring both overall rankings and the strengths and weaknesses within each region.



Global Cybersecurity Index 2020



FIGURE 3.2

The **MENA** region exhibits commendable commitment with two nations, **Saudi Arabia and UAE, in the global top 10**, emphasising cybersecurity as a regional priority. Over the years, UAE has increased its efforts by establishing a Cyber Security Council and adopting cybersecurity standards for government agencies. Saudi too got into the bandwagon by establishing National Cybersecurity Agency (NCA) to protect the country's national security, critical infrastructure, and government services. Nevertheless, the variance between leading countries and others calls for concerted efforts to ensure a more uniform cybersecurity posture.

In **South America, Brazil takes the lead on the global stage**, showcasing a robust cybersecurity position. It jumped from 71st position in 2018 to 18th position in 2020 according to the ITU report. This is because of the combined efforts of both government and private bodies in cybersecurity, collectively investing around \$1.7B in 2023. Meanwhile Argentina and other regional counterparts indicate an opportunity for collaborative efforts to enhance overall cybersecurity preparedness.

In **Southeast Asia, Singapore stands out as a global leader in cybersecurity**. It does not only have a Cybersecurity Code of Practice (CCoP) for Critical Information Infrastructure (CII) but also Cyber Security Group (CSG) to protect the government's ICT&SS (Smart Systems) and to build a trusted digital government. Indonesia and the Philippines, poised for growth, stand to gain immensely through the exchange of knowledge and collaborative resource-sharing.

Moreover, these regions have implemented region-specific regulatory frameworks, supported by dedicated regulatory bodies, comprehensive cybersecurity strategies, and stringent laws addressing cybercrime and data protection.



Cybersecurity Measures Implemented in Emerging Markets



**Cybercrime
Law**



**Data Protection
Law**



**Cybersecurity
Strategy**



**Cybersecurity
Organisation**



The key cybersecurity measures implemented across various emerging markets, focuses on four crucial segments: Cybercrime Law, Data Protection Law, Cyber Security Strategy, and Cyber Security Organisations.

Cybercrime Law:

The implementation of cybercrime laws is a cornerstone in addressing digital threats. Most countries in our examination have established such laws between 2011 and 2018, signifying a growing recognition of the need for legal frameworks to combat cybercrime. However, exceptions like Singapore (1993), Malaysia (1997), and Indonesia (2008) as shown in fig 6 highlight a historical awareness in certain regions, underlining the evolving nature of cybersecurity awareness.

Data Protection Law:

The landscape of data protection laws exhibits a wider variation. Some countries, including Bahrain, Kuwait, and Qatar, have enacted data protection laws more recently (2019 onwards), indicating an emerging consciousness of data privacy. In contrast, countries like Singapore (2012) and Thailand (2007) boast a longer history of legal frameworks, emphasising a non-uniform pace in legal development across emerging markets.

Cyber Security Strategy:

National cybersecurity strategies are crucial as they are the main documents of nation states to set strategic principles, guidelines, and objectives and in some cases specific measures to mitigate risk associated with cybersecurity. Most countries in our analysis have developed such strategies, with implementation dates ranging from 2010 (Oman) to 2023 (Indonesia). However, the diverse implementation timelines suggest that while some countries have mature strategies, others are still in the early stages of this crucial process.

Cyber Security Organisations:

Establishing dedicated cybersecurity organisations, exemplified by entities like NCSC-BH (Bahrain), CERT-PH (Philippines), and LGPD (Brazil), signifies a global commitment to operationalising cybersecurity measures. Despite progress in cybercrime laws, data protection, and national strategies, diverse timelines and development levels underscore the dynamic nature of cybersecurity awareness, allowing room for further evolution.



Cybersecurity Measures in Emerging Markets


















	 Bahrain	 Kuwait	 Oman	 Qatar	 KSA	 UAE	 Egypt	 Malaysia	 Indonesia	 Vietnam	 Thailand	 Philippines	 Brazil	 Argentina	 Nigeria	 Kenya	 Morocco
Cybercrime Law	2014	2015	2011	2014	2015	2012	2018	1997	2008	2015	2007	2012	2012	2008	2015	2018	2022
Data Protection Law	PDPL, 2019	DPPR, 2021	PDPL, 2023	DPL, 2017	PDPL, 2021	PDPL, 2021	DPL, 2020	PDPA, 2011	PDP, 2022	PPD, 2023	PDPA, 2019	DPA, 2012	LGPD, 2020	PDPL, 2001	NDPA, 2023	DPA, 2019	DLA, 2009
Cybersecurity Strategy	2017	2017	2010	2014	2013	2019	NA	2020	2023	2022	2017	2017	2020	2019	2021	2022	2020
Cybersecurity Organisations	NCSC-BH	CITRA	OCERT	QCERT	NCSC	TDRA	EG-CERT	NACSA	BSSN	NCSC	NCSA	CERT-PH	DICS	DPA	CSEAN	KE-CIRT/CC	DGSSI

FIGURE 3.3

Most of the countries have implemented cybercrime laws between 2011 and 2015. Bahrain, Kuwait, and Oman are the exceptions, having implemented such laws in 2014, 2015, and 2011, respectively. Malaysia is the earliest adopter, with a cybercrime law dating back to 1997.

Technological Frontiers in Cybersecurity Space

In a recently published report by the World Economic Forum¹ in January 2023, a striking convergence was observed between business and cyber leaders in their outlook on emerging technologies. Notably, **organisational leaders acknowledged the swift implementation of various emerging technologies, particularly in fields like machine learning**, which is increasingly permeating a diverse array of processes, thereby shaping the cyber-risk landscape for their organisations.

Among the key findings, artificial intelligence (AI) and machine learning emerged as the foremost influencers on cyber risk strategies, with 20% of respondents highlighting their impact. Following closely were the broader adoption of cloud technology (19%) and advancements in user identity and access management (15%).

Notably, respondents didn't rank other emerging technologies significantly lower than the top three, indicating a holistic approach to implementation. **This emphasises the need for integrating cyber-risk management throughout the entire digital transformation process.**



Solutions within the Cybersecurity Domain

In a rapidly evolving digital landscape where cyber threats continually escalate in sophistication, the demand for robust cybersecurity solutions has never been more critical. As organisations face a dynamic array of challenges, venture funding for cybersecurity startups becomes a pivotal indicator of industry trends and innovation.

According to Crunchbase¹, venture funding for cybersecurity startups in Q3 exhibited a modest increase from Q2, recording nearly \$1.9 billion raised across 153 deals, marking a 12% growth from the previous quarter. However, compared to the same quarter the previous year, the figures indicate a substantial decline of 30%, with Q3 2023 falling short of the \$2.7 billion raised in Q3 2022, accompanied by a 17% decrease in deal flow.

Let's delve into the key segments:

Fraud & Identity Management:

To secure online transactions by identifying and preventing fraudulent activities. Startups like Uqudo and Acronis, utilises machine learning algorithms to proactively detect and mitigate fraud, ensuring the integrity of financial transactions and user interactions. This is also the most populated segment in the cybersecurity market.



Mobile Threat Protection:

To safeguard mobile devices and applications. Cloud-based platforms and predictive technology companies such as Appthority and Skycure are employed to automatically identify and grade risky behaviour in mobile apps, protecting users from known and unknown malware and targeted attacks.

Security orchestration, automation, and response (SOAR):

Startups like Spire and Demisto use automation, natural language processing, and massive-scale endpoint protection to streamline security tasks. This enables security and IT operations teams to efficiently manage and respond to potential threats across the enterprise.

Cyber-Risk Consultations:

Encompasses companies ranging from those focused on cyber-insurance to those emphasising security policy and compliance. The goal is to provide solutions that help organisations understand, quantify, and manage cyber risks in the context of financial impact and compliance requirements.

App Security:

In this category, the focus is on securing specific enterprise applications rather than entire networks. Startups provide frameworks and solutions to help developers identify, fix, and monitor vulnerabilities in web-based, mobile, and network applications.

IoT Security:

Startups in IoT security develop AI-powered solutions to protect the safety, security, and reliability of the Internet of Things. These solutions detect and mitigate threats to IoT devices, ensuring the integrity of connected systems. Companies like Bastille Networks utilises machine learning algorithms to secure the IoT on corporate campuses by identifying airborne threats such as hidden recording devices or transmitters in a conference room, and allow for a pre-emptive response to data theft.

Deception Security:

Involves proactively deceiving and disrupting ongoing cyber-attacks. Companies like Scalefusion and Sceptrio create deceptive environments using neural networks comprising numerous fictitious computers, devices, and services to confuse and thwart attackers, adding an additional layer of defence.













Cybersecurity Solutions in Emerging Markets











Fraud and Identity Management

Country	Companies
UAE 	Uqudo 
Egypt 	GateLock Technology VAD 
Philippines 	Netrust 
Kuwait 	Shaarait 
KSA 	Exa Information Technology 
Vietnam 	Wee Digital 
Singapore 	Acronis 
Malaysia 	i-Sprint 
Brazil 	Apura 









Mobile Threat Protection

Country	Companies
USA 	Appthority 
USA 	Mi3 Security 
USA 	Sentigrity 
USA 	Skycure 
USA 	Zimperium 

IoT Security

Country	Companies
USA 	Cujo 
USA 	Bastille 
USA 	SparkCognition 
Germany 	Infineon Tech 
Singapore 	Itsec.asia 

App Security

Country	Companies
India 	Authbase 
France 	Cryptosense 
Singapore 	Ensign InfoSecurity 
Thailand 	MonitoringLabs 

Deception Technology

Country	Companies
Canada 	Scalefusion 
UAE 	Spire Solutions 
Singapore 	Sectrio 

FIGURE 3.4

Cybersecurity Solutions in Emerging Markets

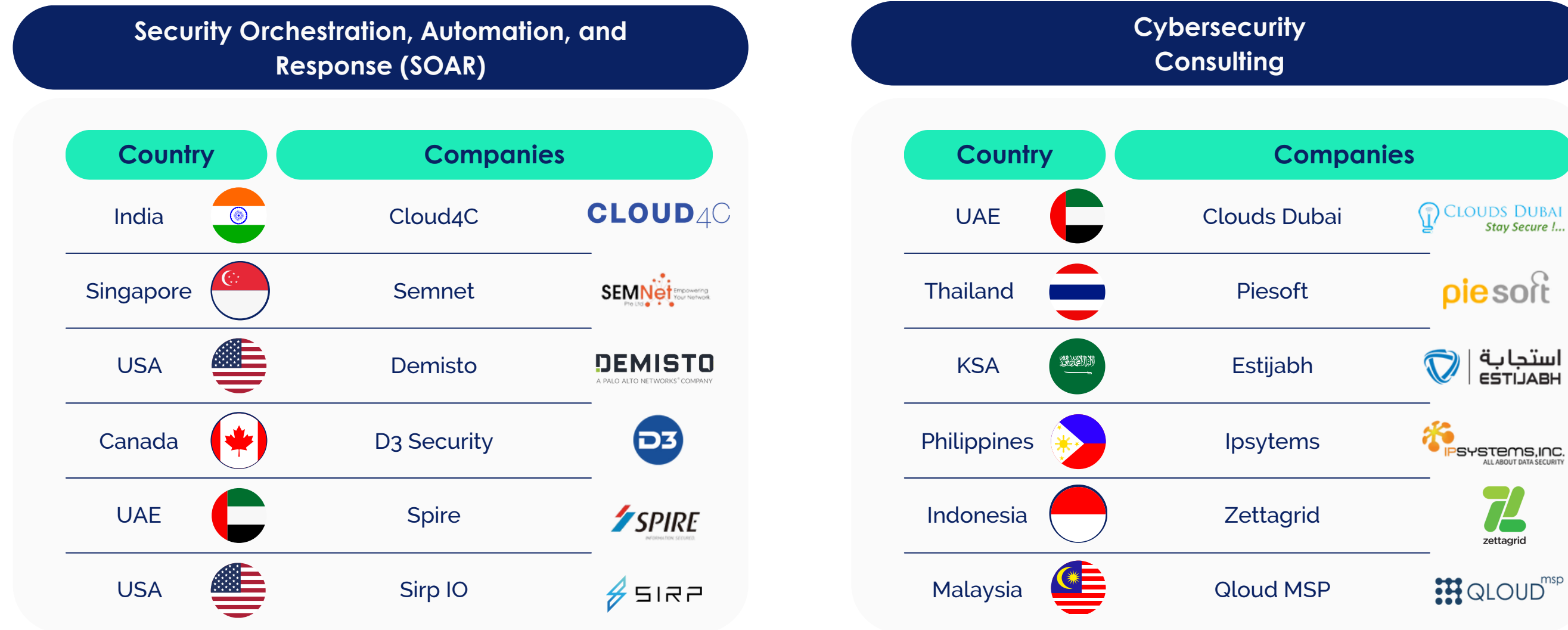


FIGURE 3.4

As organisations navigate the ever-evolving technological landscape, **strategic foresight and proactive cyber-risk management will be paramount.** The varying solutions within the cybersecurity domain demonstrate the industry's resilience and adaptability, providing a diverse toolkit for safeguarding against an array of digital threats.

In essence, the cybersecurity journey is an ongoing narrative, with startups playing a crucial role in developing cutting-edge solutions. As we move forward, the collaboration between industry leaders, innovative startups, and policymakers will be essential to fortify our digital future against emerging cyber challenges.

What are the Industry Leaders Saying?

“While organisations are taking steps to better align cybersecurity programs with business goals, there is still plenty of room for improvement, with more than 60% of respondents still falling victim to successful breaches coming from outside their organisation. Working more effectively across the C-suite and ensuring that security efforts have a positive business impact require a business-led CISO who acts as an educator and collaborator with non-security leaders.

Jacky Fox¹
Security lead for Europe


accenture



Key Takeaways and Future Outlook



In navigating the intricate landscape of cybersecurity within the Banking and Financial Services Industry (BFSI), a comprehensive understanding of emerging trends, challenges, and strategic responses is paramount. As the global market continues to evolve, the BFSI sector grapples with escalating cyber threats, digital transformation imperatives, and the growing awareness to fortify financial operations.

The evolution of cyber threats from 1975 to 2023 reveals a pronounced shift in focus towards the banking sector, especially in emerging markets. The finance and insurance industry faced a significant brunt, accounting for 18.9% of cyber-attacks in 2022. This trend underscores the **persistent targeting of financial institutions, employing sophisticated techniques such as zero-day exploits, malware, and social engineering**. These methods pose significant risks to financial data, as data breaches driven by financial gain remain prevalent across various entities in the financial sector, raising concerns about customer privacy. The COVID-19 pandemic acted as a catalyst, heightening vulnerabilities and necessitating industries to fortify digital defences in an interconnected and rapidly evolving cybersecurity landscape.

Emerging market banks are increasing cybersecurity spending due to the growing threat, driven by technological advancements like AI, IoT, Blockchain, and 5G. The BFSI sector's integration of digital technologies aims to boost operational efficiency and enhance customer experiences, with cybersecurity investments showing a robust 16% CAGR from 2014 to 2018 and a projected increase in rate in the following years.

In the MENA region, Saudi Arabia and the UAE stand out as cybersecurity leaders. While in South America Brazil ranks strongly, Singapore excels in Southeast Asia. Other countries from these regions are also coming up with measures and initiatives such as increasing investments in digital space or building infrastructure, to build a secure cyber space for businesses and clients. These insights highlight the diverse cybersecurity landscape in emerging markets, necessitating regional cooperation to address varying levels of readiness.

Artificial intelligence (AI) and machine learning emerge as pivotal technologies shaping cyber risk strategies, with 20% of respondents acknowledging their impact. Cloud technology follows closely at 19%, and advancements in user identity and access management are noted by 15%, reflecting a holistic approach to technology adoption. Simultaneously, Q3 2023 witnessed a 12% increase in venture funding for cybersecurity startups, reaching almost \$1.9 billion, though a notable 30% decline compared to Q3 2022 signals a nuanced funding landscape.



As organisations navigate complex technology landscapes, **strategic foresight and proactive cyber-risk management are crucial**. Leading banks are leveraging biometric technology for streamlined logins. One example is HSBC¹ who is leveraging biometric technology for streamlined logins using Apple's Touch ID and HSBC Voice ID across 18 markets. The idea is that while Voice authentication is more secure than other authentication methods because it uses a person's unique voiceprint, Touch ID fingerprints are stored on the device and cannot be accessed by any mobile apps. What's more - in 2022, DBS² launched a free cybersecurity training programme aimed at safeguarding Singapore's SME community, consisting of 280,000 businesses, against the increasing threat of cybercrime. At the end of the programme, SMEs were given tailored advice on appropriate cyber insurance and cybersecurity solutions, empowering them to promptly fortify their businesses against potential cyber threats.

The cybersecurity journey is continuous, with startups making significant contributions to cutting-edge solutions. However, the real-world impact is evident in incidents like the high-profile data breach that happened at JP Morgan Chase that led to substantial financial losses for individuals. In such instances, although businesses may bear the brunt of data breaches, the true cost extends far beyond the corporate realm. Clients not only lose sensitive information but also face tangible financial setbacks, jeopardising their plans for significant life milestones. The aftermath of a breach resonates in the pockets of individuals who may have earmarked those funds for their first home, dream car, or crucial monthly payments like EMIs.

These incidents not only deepen the critical need for robust cybersecurity measures but also stresses the very real and human consequences of lapses in data protection. As organisations navigate the intricate technological terrain, strategic foresight and proactive cyber-risk management are vitally important.

¹ The Guardian. (2016, February 19). HSBC Rolls Out Voice and Touch ID Security for Bank Customers. Retrieved Nov 2023, from <https://www.theguardian.com/business/2016/feb/19/hsbc-rolls-out-voice-touch-id-security-bank-customers>

² DBS Bank. (2022). DBS Rolls Out Complimentary Cybersecurity Training to Help Inoculate Singapore's 280,000 SMEs Against Cybercrime. Retrieved Nov 2023, from https://www.dbs.com/newsroom/DBS_rolls_out_complimentary_cybersecurity_training_to_help_inoculate_Singapores_280000_SMEs_against_cybercrime#:~:text=This%20enables%20SMEs%20to%20take,security%2C%20and%20social%20media%20security



Citations

Cybersecurity in the Banking Industry

Figure 2.1

- Malwarebytes. (n.d.). Trojan. Retrieved from <https://www.malwarebytes.com/trojan#:~:text=A%20program%20called%20ANIMAL%2C%20released,other%20users%20could%20find%20it.>
- Okta. (n.d.). Morris Worm: A Landmark in Cybersecurity History. Retrieved from <https://www.okta.com/identity-101/morris-worm/#:~:text=A%20hacker%20launched%20the%20Morris,worm%20inspired%20generations%20of%20hackers.>
- Wikipedia. (n.d.). Ransomware. Retrieved from <https://en.wikipedia.org/wiki/Ransomware#:~:text=History%20of%20malware-,Encrypting%20ransomware,pay%20the%20extortionist%20at%20all.>
- Wikipedia. (n.d.). ILOVEYOU. Retrieved from <https://en.wikipedia.org/wiki/ILOVEYOU.>
- Wikipedia. (n.d.). Melissa (computer virus). Retrieved from [https://en.wikipedia.org/wiki/Melissa_\(computer_virus\).](https://en.wikipedia.org/wiki/Melissa_(computer_virus).)
- Encyclopedia Britannica. (n.d.). Denial-of-Service Attack. Retrieved from <https://www.britannica.com/technology/denial-of-service-attack#:~:text=The%20first%20documented%20DoS%2Dstyle,sites%2C%20including%20Amazon%20and%20eBay.>
- Allot. (2020). Cryptojacking: A Rising Threat. Retrieved from https://www.allot.com/resources/TB_Cryptojacking.pdf.

Figure 2.2

- Carnegie Endowment. (2022). Timeline of Cyber Incidents Involving Financial Institutions. Retrieved from <https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline>

Figure 2.3

- CB Insights. (2020). Top banks cybersecurity investments expert intelligence. Retrieved from <https://www.cbinsights.com/research/top-banks-cybersecurity-investments-expert-intelligence/>

Figure 2.4

- Statista. (2022). Cyber security venture capital funding worldwide from 2017 to 2022. Retrieved from <https://www.statista.com/statistics/1287802/cyber-security-vc-funding-worldwide/>

Cybersecurity Landscape in Emerging Markets

Figure 3.1

- Statista. (2022). Distribution of cyber-attacks across worldwide industries in 2022. Retrieved from <https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/>

Figure 3.2

- International Telecommunication Union. (2021). Global Cybersecurity Index (GCI): Methodology and questionnaire (Edition 01 - 2021). Retrieved January 4, 2024, from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Figure 3.3

- National Cyber Security Centre (Bahrain). (n.d.). Retrieved from <https://www.ncsc.gov.bh/en/index.html>
- CITRA (Communications and Information Technology Regulatory Authority, Kuwait). (n.d.). Cybersecurity. Retrieved from <https://citra.gov.kw/sites/en/Pages/cybersecurity.aspx>
- Oman Portal. (n.d.). Retrieved from <https://omanportal.gov.om/wps/wcm/connect/EN/site/home/cr/cr8lss/cr82/>
- Q-CERT (Qatar Computer Emergency Response Team). (n.d.). Retrieved from <https://www.qcert.org/>
- Government of Saudi Arabia. (n.d.). National CyberSecurity Authority. Retrieved from https://www.my.gov.sa/wps/portal/snp/agencies/agencyDetails/AC403!/ut/p/z0/04_SjgCPykssyoxPLMnMzovMAfjjo8zivQlsTAwdDQzgLQwNzQwCnSotXPwMvYwNDAzog1PzgL3oo_ArAppiVOTr7JuuH1WQWJkHm5mXlq8f4ehsYmCsX5DtHg4Aml1fKQ!!/



Citations

- Telecommunications and Digital Government Regulatory Authority (TDRA), UAE. (n.d.). National Cybersecurity Strategy. Retrieved from <https://tdra.gov.ae/Pages/Error500.html?aspxerrorpath=/en/national-cybersecurity-strategy>
- Ministry of Communications and Information Technology (MCIT), Egypt. (n.d.). Cyber Security. Retrieved from https://mcit.gov.eg/en/TeleCommunications/Industry/Cyber_Security
- Cyber Security Agency of Singapore. (2021). Singapore Cybersecurity Strategy 2021. Retrieved from <https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021>
- National Cyber Security Agency (NACSA), Malaysia. (n.d.). Retrieved from <https://www.nacsa.gov.my/about-us.php>
- Indonesian Security Incident Response Team on Internet Infrastructure (ID-SIRTII/CC). (n.d.). Retrieved from https://idsirtii.or.id/en/bssn_page.html
- Cybersecurity Intelligence. (n.d.). National Cyber Security Center (NCSC) Vietnam. Retrieved from <https://www.cybersecurityintelligence.com/national-cyber-security-center-ncsc-vietnam-8194.html>
- Cybersecurity Intelligence. (n.d.). National Cyber Security Agency (NCSA) - Thailand. Retrieved from <https://www.cybersecurityintelligence.com/national-cyber-security-agency-ncsa---thailand-9852.html>
- National Computer Emergency Response Team (NCERT), Philippines. (n.d.). Retrieved from <https://www.ncert.gov.ph/about-us/ncert/>
- Cyber Security Experts Association of Nigeria (CSEAN). (n.d.). Retrieved from <https://csean.org.ng/#:~:text=CSEAN%20%E2%80%93%20CSECYBER%20SECURITY%20EXPERTS%20ASSOCIATION%20OF%20NIGERIA%20%E2%80%93%20Professionals%20in%20Cybersecurity>
- Communications Authority of Kenya. (n.d.). Cyber Security. Retrieved from <https://www.ca.go.ke/cyber-security#:~:text=The%20National%20KE%2DCIRT%2FCC,Authority%20and%20law%20enforcement%20agencies>
- Direction Générale de la Surveillance du Territoire et de l'Information (DGSSI), Morocco. (n.d.). Retrieved from <https://www.dgssi.gov.ma/>
- Personal Data Protection Authority, Bahrain. (n.d.). Retrieved from <http://www.pdp.gov.bh/en/index.html>
- SecurePrivacy AI. (n.d.). Oman Data Protection Law. Retrieved from <https://secureprivacy.ai/blog/oman-data-protection-law#:~:text=The%20Oman%20Personal%20Data%20Protection,there%20is%20another%20legal%20basis>
- Chambers Practice Guides. (2023). Data Protection & Privacy 2023 - Qatar. Retrieved from <https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2023/qatar#:~:text=1.1%20Laws,East%20to%20introduce%20the%20DPL>
- Saudi Data and Artificial Intelligence Authority. (2023). Personal Data Protection Regulation. Retrieved from <https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf>
- Communications and Information Technology Regulatory Authority, Kuwait. (n.d.). Data Privacy Protection Regulation. Retrieved from https://www.citra.gov.kw/sites/en/LegalReferences/Data_Privacy_Protection_Regulation.pdf
- PwC Middle East. (n.d.). Egypt Data Protection Law. Retrieved from <https://www.pwc.com/m1/en/services/consulting/technology/cyber-security/navigating-data-privacy-regulations/egypt-data-protection-law.html#:~:text=The%20Egyptian%20Law%20No.,published%20within%20the%20next%20year>
- United Arab Emirates Government. (n.d.). Data Protection Laws. Retrieved from <https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws>
- National Privacy Commission, Philippines. (n.d.). Data Privacy Act. Retrieved from <https://privacy.gov.ph/data-privacy-act/>
- Malaysia Government. (n.d.). Personal Data Protection Act. Retrieved from <https://www.malaysia.gov.my/portal/content/654>
- Thales Group. (n.d.). Indonesia Personal Data Protection Law. Retrieved from [https://cpl.thalesgroup.com/compliance/apac/indonesia-personal-data-protection-law#:~:text=The%20Personal%20Data%20Protection%20\(PDP,October%2017%2C%202022%20in%20Indonesia\)\(https://cpl.thalesgroup.com/compliance/apac/indonesia-personal-data-protection-law#:~:text=The%20Personal%20Data%20Protection%20\(PDP,October%2017%2C%202022%20in%20Indonesia\)](https://cpl.thalesgroup.com/compliance/apac/indonesia-personal-data-protection-law#:~:text=The%20Personal%20Data%20Protection%20(PDP,October%2017%2C%202022%20in%20Indonesia)(https://cpl.thalesgroup.com/compliance/apac/indonesia-personal-data-protection-law#:~:text=The%20Personal%20Data%20Protection%20(PDP,October%2017%2C%202022%20in%20Indonesia))
- Securiti. (n.d.). Vietnam Personal Data Protection Decree. Retrieved from <https://securiti.ai/vietnam-personal-data-protection-decree/#:~:text=I.,Introduction,enacted%20on%20April%2017%2C%202023>
- DLA Piper. (n.d.). Brazil - LGPD (Lei Geral de Proteção de Dados). Retrieved from <https://www.dlapiperdataprotection.com/index.html?t=law&c=BR#:~:text=The%20LGPD%20is%20Brazil's%20first,enforceable%20on%20August%201%2C%202021>
- DLA Piper. (n.d.). Argentina - PDPL (Personal Data Protection Law). Retrieved from <https://www.dlapiperdataprotection.com/index.html?t=law&c=AR#:~:text=Law%202025%2C326%20%2D%20the%20Personal%20Data,regulations%20issued%20under%20the%20PDPL>
- DataGuidance. (2023). Nigeria Data Protection Overview. Retrieved from <https://www.dataguidance.com/notes/nigeria-data-protection-overview#:~:text=September%202023-,1.,Nigeria's%20main%20data%20protection%20legislation>
- Office of the Data Protection Commissioner, Kenya. (n.d.). Data Protection Act. Retrieved from <https://www.odpc.go.ke/dpa-act/>
- DLA Piper. (n.d.). Morocco - Data Protection. Retrieved from <https://www.dlapiperdataprotection.com/index.html?t=law&c=MA>





As a corporate training and consulting provider, LeanTech SG is on a mission to develop tech-savvy leaders and create dynamic digital cultures that drives success. We help organisations lean on tech to combat disruption with confidence and become digitally transformed.

Advance your digital journey with us today.

Contact Us

info@leantech.sg

+65 3138 3778 (Headquarters)

+971 58 598 3974 (UAE Office)



[leantechsg](https://www.linkedin.com/company/leantechsg)



[LeantechSG](https://twitter.com/LeantechSG)



www.leantech.sg