Cybersecurity Trends in Thailand

A Comprehensive Analysis for 2024-2025

1. Executive Summary

The cybersecurity landscape in Thailand is undergoing a period of significant transformation, marked by rapid market growth, an evolving threat environment, proactive government initiatives, increasing adoption of advanced security solutions, a persistent skills gap, and the influence of global and regional geopolitics. This analysis provides a comprehensive overview of these key trends for 2024 and 2025, highlighting the challenges and opportunities for businesses, government agencies, and cybersecurity professionals operating within the Kingdom. The Thai cybersecurity market is experiencing robust expansion, driven by the nation's accelerating digital transformation and the escalating sophistication of cyber threats. While the government has established a foundational regulatory framework and is actively pursuing initiatives to bolster the country's cyber defenses and address the critical skills shortage, organizations continue to face a diverse array of cyber threats, ranging from prevalent phishing attacks to emerging AI-powered intrusions. The adoption of advanced security solutions like zero-trust architecture and extended detection and response (XDR) is gaining momentum, yet challenges remain in achieving widespread and mature implementation. Geopolitical factors, particularly the increasing reliance on digital infrastructure from specific nations, also play a crucial role in shaping Thailand's cybersecurity posture. Looking ahead, the threat landscape is expected to become even more complex, necessitating a collaborative and proactive approach from all stakeholders to ensure a secure digital future for Thailand.

2. Thailand Cybersecurity Market Analysis (2024-2025)

The cybersecurity market in Thailand is demonstrating strong growth, reflecting an increasing awareness of the importance of digital security in the face of evolving threats. Projections from Mordor Intelligence indicate a substantial expansion, with the market size anticipated to grow from USD 508.89 million in 2025 to USD 984.12 million by 2030, registering a compound annual growth rate (CAGR) of 14.10%.[1] This robust growth trajectory signifies a rising level of investment in cybersecurity solutions and services across various sectors in Thailand. Simultaneously, analysis by Nucamp presents a similar outlook, estimating the market size at USD 446 million in 2024 and projecting a rise to nearly USD 872 million by 2029, also with a CAGR of 14.10%.[2] The consistency in the projected CAGR from these independent sources underscores a strong and stable growth trend within the Thai cybersecurity market, suggesting a fundamental market dynamic driving this expansion. The near doubling of the market size within a five-year span further emphasizes the rapid digitization occurring in Thailand and the corresponding escalating need for robust cybersecurity measures to protect digital assets and infrastructure.[2] This growth presents significant opportunities for cybersecurity vendors, service providers, and professionals to cater to the increasing demand for their expertise.

In addition to these market size projections, Gartner's forecast focuses on end-user spending on information security in Thailand, anticipating it to reach THB 18.4 billion (approximately USD 500-520 million based on current exchange rates) in 2025. This represents a 12.3% increase from the estimated spending of THB 16.4

billion in 2024.[3] While Gartner's projected growth rate is slightly lower than the 14.10% CAGR indicated by Mordor Intelligence and Nucamp, it still signifies a substantial year-over-year increase in cybersecurity spending by organizations within Thailand. This difference in growth rate could potentially stem from Gartner's specific focus on end-user spending, which might exclude other segments of the cybersecurity market such as government investments or spending by cybersecurity service providers themselves. Nevertheless, the consistent upward trend across these forecasts confirms that organizations in Thailand are increasingly allocating budgets to bolster their cybersecurity defenses.

Several key factors are driving the expansion of the cybersecurity market in Thailand. The increasing demand for digitalization and scalable IT infrastructure across various sectors is a primary driver.[1] As Thailand embraces digital transformation to enhance efficiency, improve services, and drive economic growth, the need for secure and scalable IT infrastructure becomes paramount. This expanding digital footprint introduces new vulnerabilities and attack surfaces, thereby directly fueling the demand for robust cybersecurity solutions capable of protecting these evolving digital environments. Furthermore, the need to tackle evolving cyber threats, including the complexities of managing third-party risks and the growing adoption of cloud-first strategies, is compelling organizations to invest in more advanced cybersecurity measures.[1] Traditional security approaches are often proving inadequate against the sophistication and frequency of modern cyberattacks, necessitating the adoption of more sophisticated tools, strategies, and expertise to secure increasingly complex IT ecosystems.

Government initiatives also play a crucial role in shaping the cybersecurity market in Thailand. Policies promoting digitalization and cloud adoption, such as the "Go Cloud First" initiative, are driving the adoption of digital technologies across government agencies and businesses.[1] This increased reliance on digital platforms and services inherently creates a greater need for robust cybersecurity measures to safeguard sensitive data and critical operations. Moreover, the rising number of cyberattacks against both public and private organizations in Thailand serves as a stark reminder of the ever-present risks in the digital landscape.[1] Real-world incidents of data breaches, ransomware attacks, and other cybercrimes often serve as catalysts for increased awareness and a greater willingness to invest in cybersecurity solutions to prevent future incidents and mitigate potential damage.

Spending trends within the Thai cybersecurity market further illustrate the evolving priorities of organizations. A projected 15% rise in security software spending in 2025 is anticipated, largely driven by the increasing need to address cybersecurity challenges posed by the growing adoption of Generative AI technologies.[3] This significant increase in security software spending indicates a proactive approach by Thai organizations to confront emerging threats, particularly those associated with AI. It suggests a growing understanding of the potential risks that AI can introduce and a corresponding willingness to invest in AI-powered security solutions to enhance their defenses. Furthermore, the cloud security segment is expected to witness exponential growth within the Thai cybersecurity market, fueled by the ongoing shift towards cloud-based delivery models.[1] As more businesses in Thailand migrate their operations and data to the cloud to leverage its scalability and flexibility, the need to secure these cloud environments becomes a paramount concern, driving increased investment in cloud-specific security solutions and expertise.

The competitive landscape of the cybersecurity market in Thailand is characterized by the strong presence of major global players such as Palo Alto Networks, Cisco Systems, Fortinet, Check Point Software

Technologies, and Kaspersky.[6] These established international vendors bring a wealth of global expertise and cutting-edge technologies to the Thai market, often holding significant market share due to their established reputation and comprehensive security portfolios. These leading companies are strategically focusing on key areas such as AI-enhanced threat intelligence, Zero Trust Architecture, and the development of strategic partnerships to further enhance their market positions within Thailand.[6] This focus on advanced technologies indicates the direction in which the Thai cybersecurity market is evolving, with a growing demand for proactive and sophisticated security approaches capable of addressing the increasingly complex threat landscape.

To provide a clearer overview of the market's growth trajectory, the following table summarizes the Thailand Cybersecurity Market Size and Growth Forecasts from various sources for 2024-2030:

Source	Year	Market Size (USD Million)	CAGR (2025-2030)
Nucamp	2024	446	14.10%
Mordor Intelligence	2025	508.89	14.10%
Gartner	2025	~500-520	~12.3%
Nucamp	2029	872	N/A
Mordor Intelligence	2030	984.12	N/A

This table illustrates the consistent growth expected in the Thai cybersecurity market over the coming years, highlighting the significant opportunities for stakeholders in this dynamic sector.

3. Current Cybersecurity Threat Landscape in Thailand

Thailand's digital landscape is facing a complex and evolving array of cybersecurity threats, posing significant challenges to organizations and individuals alike. Among the most prevalent threats observed in 2024 and expected to continue into 2025 are phishing and social engineering attacks [2, 2, 8, 9, 10, 28, 8]. These deceptive tactics remain highly effective in exploiting human vulnerabilities to gain unauthorized access to sensitive information or systems. The increasing sophistication of these attacks, often leveraging AI to create more convincing and personalized lures, underscores the critical need for ongoing user awareness training programs and the implementation of robust email security measures within Thai organizations.

Malware, encompassing various forms such as viruses, worms, and ransomware, also continues to represent a significant threat to cybersecurity in Thailand [2, 2, 8, 9, 10, 8, 1, 7]. These malicious software programs can cause substantial damage, including data breaches, financial losses, and disruptions to critical operations. The persistence of malware attacks necessitates the deployment of strong endpoint protection

solutions, coupled with effective incident response capabilities to quickly detect, contain, and eradicate infections.

A concerning trend observed in 2024 is the surge in the trafficking of sensitive personal data on the dark web.[7] This illicit activity highlights the increasing value that cybercriminals place on stolen personal information, which can be subsequently used for various malicious purposes, including identity theft and financial fraud. The rise of data trafficking underscores the importance of implementing stringent data protection measures and proactively monitoring for compromised credentials to mitigate the risk of data breaches and their exploitation.

The emergence and growing sophistication of AI-powered cyberattacks are also becoming a significant concern in Thailand.[8] Attackers are increasingly leveraging artificial intelligence to create more personalized and evasive phishing campaigns, develop malware that can adapt to security defenses, and even target critical infrastructure. The rise of these AI-driven threats necessitates that organizations in Thailand adapt their security strategies and invest in AI-powered security solutions for enhanced detection and response capabilities.

Banking fraud and the use of banking malware are notably more prevalent in Thailand compared to the global average.[9] This indicates that financial institutions and their customers in Thailand are particularly vulnerable to these types of cyber threats, requiring the implementation of enhanced security measures specific to the financial sector. This includes stronger authentication protocols, advanced transaction monitoring systems, and public awareness campaigns aimed at educating individuals on how to avoid becoming victims of online financial fraud.

The 2024 ThaiCERT report provides further insights into the common types of cyberattacks experienced in Thailand, identifying fake websites and URLs, data theft, and disruption of services as the top categories.[12] This broad spectrum of attack types suggests that organizations in Thailand are facing a multifaceted threat landscape, requiring the adoption of comprehensive security strategies that can address various attack vectors, from social engineering tactics to technical exploits targeting system vulnerabilities.

The primary threat actors operating within Thailand's cybersecurity landscape include cybercriminals, who are primarily motivated by financial gain through activities such as ransomware attacks, banking fraud, and the theft and sale of sensitive data.[13] Additionally, nation-state actors are also active in the region, potentially engaging in cyber espionage targeting government entities, critical infrastructure, and organizations holding sensitive national security information.[11] The presence of both financially motivated cybercriminals and sophisticated state-sponsored actors creates a complex and challenging threat environment for Thailand.

Several sectors in Thailand have been identified as key targets for cyberattacks. These include finance and banking, commerce, foreign commerce, retail, IT and telecom, healthcare, and energy.[4] The targeting of critical infrastructure sectors such as finance, energy, and healthcare is particularly concerning, as successful cyberattacks against these sectors could lead to significant disruptions with far-reaching consequences for the Thai economy and society.

4. Government Initiatives and Regulatory Framework

The government of Thailand has recognized the growing importance of cybersecurity and has established a foundational legal and regulatory framework to address the evolving threat landscape. A key piece of legislation in this regard is the Cybersecurity Act of 2019.[16] This act provides a comprehensive legal basis for addressing cybersecurity threats, outlining the roles and responsibilities of various government agencies and stakeholders in protecting the nation's digital infrastructure and ensuring a coordinated national response to cyber incidents.

Furthermore, the Personal Data Protection Act (PDPA) mandates that organizations handling personal data in Thailand implement specific security measures to protect this information.[2] The PDPA also requires organizations to appoint data protection officers and conduct regular security checks, driving a greater focus on data privacy and security practices across the country.

Recognizing the increasing reliance on cloud computing, the Thai government has also established Cybersecurity Standards for Cloud Systems B.E. 2567 (2024).[16] These standards provide comprehensive guidelines for securing cloud systems used by government agencies, regulators, and organizations designated as critical information infrastructure under the Cybersecurity Act. This initiative reflects the government's commitment to ensuring the security of cloud environments, particularly within the public sector and critical infrastructure.

To combat online financial fraud, the Cybercrime Decree of 2023 empowers victims to promptly freeze suspicious transactions.[2] This measure provides a crucial mechanism for rapid response to financial cybercrime, potentially mitigating the financial impact on individuals and disrupting the illicit activities of cybercriminals.

The Thai government has also implemented updated measures in 2024 aimed at accelerating the monitoring and blocking of illegal online content.[2] Additionally, penalties for data trading have been increased, demonstrating the government's ongoing efforts to adapt to the evolving cyber threat landscape by enhancing its enforcement capabilities and deterring illegal activities in the digital realm.

Several government agencies are actively involved in strengthening Thailand's cybersecurity posture. The National Cyber Security Agency (NCSA) serves as the central body responsible for national cybersecurity strategy and implementation.[1] The NCSA plays a crucial role in strengthening national cybersecurity measures, assessing cybersecurity risks within government agencies, and driving reforms to existing cybersecurity laws to ensure they remain effective in addressing emerging threats.

In a significant initiative to address the critical cybersecurity skills gap in Thailand, the NCSA has partnered with ISC2 to train 10,000 new cybersecurity professionals by 2026, offering free training and certification programs.[2] This ambitious program aims to significantly increase the pool of qualified cybersecurity professionals available to organizations across various sectors in Thailand.

The Thai government is also embracing advanced technologies like AI and robotic process automation to enhance its own security operations and improve efficiency in detecting and responding to cyber threats.[2] Furthermore, the "Go Cloud First" initiative demonstrates the government's commitment to promoting the

adoption of cloud technologies across the public sector, while also emphasizing the importance of secure cloud migration and implementation.[1] The Digital Economy and Society (DES) Ministry also plays an active role in addressing various cybersecurity issues, underscoring the government's recognition of cybersecurity as a fundamental pillar for the growth and security of Thailand's digital economy.[8]

Recognizing that cyber threats often transcend national borders, Thailand is actively engaging in international collaboration with agencies and partners such as the European Union and Japan.[16] These collaborations aim to strengthen Thailand's cyber resilience through the sharing of threat intelligence, the adoption of global best practices, and the harmonization of cybersecurity regulations. This international cooperation is considered essential for effectively combating global cybercrime and addressing transnational cyber threats.

5. Adoption of Emerging Cybersecurity Solutions

Thai organizations are increasingly recognizing the limitations of traditional security approaches in the face of a rapidly evolving threat landscape and are beginning to adopt emerging cybersecurity solutions such as zero-trust architecture and extended detection and response (XDR). A Statista survey indicates that a significant 72% of respondents in Thailand have either already adopted a zero-trust model or have concrete plans for its future implementation.[19] This high level of interest and adoption signifies a growing understanding within Thai organizations of the need to move beyond conventional perimeter-based security models towards a more granular and adaptive approach to access control and security. The increasing frequency and sophistication of cyberattacks, coupled with the rise of remote work arrangements and the widespread adoption of cloud services, are likely key factors driving this shift towards zero trust.

However, while overall adoption rates are promising, achieving a fully mature and measurable zero-trust program remains a challenge for many organizations. Gartner's prediction suggests that only around 10% of large enterprises globally will have a mature zero-trust program in place by 2026 [[30], S_S88]. This implies that while many Thai organizations are embarking on the zero-trust journey, a significant portion are likely still in the early stages of implementation, facing complexities in organizational and technological changes required for a comprehensive zero-trust architecture. Cisco's Cybersecurity Readiness Index 2024 for Thailand provides a more specific insight, revealing that 15% of organizations in the country are at the "Mature" stage of identity intelligence readiness.[20] Given that identity is a central pillar of the zero-trust model, this metric suggests that while some progress has been made in implementing key zero-trust principles, there is still considerable room for improvement across Thai organizations in achieving a mature zero-trust posture.

Extended Detection and Response (XDR) is another emerging cybersecurity solution that is gaining traction globally and holds significant potential for adoption in Thailand. The global XDR market is projected to experience a high adoption rate, driven by the increasing need for comprehensive visibility across complex IT environments and the automation capabilities that XDR offers to alleviate the burden of personnel shortages.[21] These drivers are highly relevant to the cybersecurity challenges faced by organizations in Thailand, including the growing complexity of their IT infrastructures and the persistent shortage of skilled cybersecurity professionals. The global XDR market is also forecasted to witness a substantial compound

annual growth rate (CAGR) of 39.20% between 2025 and 2034.[23] This strong projected growth indicates a significant market demand for XDR capabilities as organizations worldwide, including those in Thailand, recognize its potential to enhance their overall security posture.

The high volume of web threats observed in Thailand, with more than 28,000 incidents detected daily in 2024 [24], further underscores the potential value of XDR for Thai organizations. XDR's ability to provide enhanced visibility and faster response times by correlating security data from various sources can be particularly beneficial in managing such a high volume of threats. Moreover, Positive Technologies' analysis in 2024 identified Thailand as one of the most frequently attacked countries in Southeast Asia, accounting for 27% of attacks.[13] This high attack frequency reinforces the notion that Thai organizations are prime candidates for adopting advanced detection and response solutions like XDR to bolster their defenses and mitigate the impact of successful cyber intrusions.

The following table summarizes the adoption rates and forecasts for Zero Trust Architecture and XDR in Thailand:

Solution	Metric	Data/Forecast	Source
Zero Trust Architecture	Adoption Plans/Current Adoption	72%	Statista
Zero Trust Architecture	Mature Programs by 2026 (Global, Large Enterprises)	10%	Gartner
Zero Trust Architecture	"Mature" Stage of Identity Intelligence Readiness (Thailand)	15%	Cisco
Extended Detection Response	Global Market CAGR (2025-2034)	39.20%	MarketResearchFuture
Extended Detection Response	Thailand Web Threats per Day (2024)	>28,000	Kaspersky
Extended Detection Response	Thailand Attack Frequency in SEA (2024)	27%	Positive Technologies

This table provides a consolidated view of the current and future adoption trends for these key emerging security solutions within the context of Thailand's cybersecurity landscape.

6. The Cybersecurity Skills Gap and Capacity Building

A significant challenge facing Thailand's cybersecurity landscape is the pronounced shortage of skilled cybersecurity professionals. Recent analysis indicates that a substantial 72% of Thai organizations have reported experiencing a serious cybersecurity skills gap.[2] This shortage poses a critical impediment to the effective implementation and management of robust security measures, potentially leaving organizations more vulnerable to the increasing frequency and sophistication of cyberattacks. Furthermore, this skills gap is directly contributing to increased operational risks for the same percentage of Thai organizations.[2] The lack of qualified personnel can lead to delays in patching vulnerabilities, inadequate threat monitoring, and misconfigurations of security systems, all of which can have tangible business consequences, including disruptions to critical services, financial losses resulting from fraud or data breaches, and damage to customer trust and brand reputation.

The impact of the cybersecurity skills shortage in Thailand is further highlighted by the significantly longer average recovery time from cyberattacks compared to the global average. Thai organizations take approximately 4.3 months to recover from a cyber incident, whereas the global average stands at 2.7 months.[2] This disparity in recovery times suggests a potential lack of skilled incident responders and less mature security operations within Thailand, indicating a pressing need for more comprehensive training and investment in incident response capabilities. The effective management of cyber incidents requires specialized skills in areas such as digital forensics, malware analysis, and the implementation of containment and eradication strategies.

The skills gap is also evident within Thailand's public sector. As of September 2023, only a small fraction of Thai bureaucrats (0.5%) worked in the IT field, with an even smaller percentage specializing in information security.[1] This statistic underscores a significant deficiency in cybersecurity expertise within the government sector, which is often tasked with the critical responsibility of protecting national infrastructure and sensitive government data. A strong and well-equipped public sector cybersecurity workforce is essential for safeguarding national security and ensuring the resilience of critical services.

Recognizing the severity of the cybersecurity skills gap, several initiatives are underway in Thailand to address this critical challenge and build capacity within the sector. A significant effort is the partnership between ISC2 and Thailand's National Cyber Security Agency (NCSA) to train 10,000 new cybersecurity professionals by 2026.[2] This ambitious program offers free training and certification opportunities, aiming to lower the barrier to entry for individuals interested in pursuing careers in cybersecurity and significantly increase the pool of qualified professionals available to organizations across various industries in Thailand.

In addition to government-led initiatives, major technology companies are also stepping up to provide training programs, particularly focusing on areas such as cloud security and security operations, which are currently experiencing a high demand for skilled professionals.[2] These industry-driven training programs can help address the specific skills gaps that are most critical for organizations by providing practical, hands-on training and aligning their curriculum with the evolving needs of the cybersecurity landscape. The Thai government is also actively investing in IT programs for public sector workers and establishing partnerships with educational institutions to offer specialized training in key areas such as threat intelligence and cloud security.[16] These initiatives aim to build cybersecurity capacity within government

agencies and ensure a sustainable pipeline of future talent for the public sector. Furthermore, efforts are being made to broaden the talent pool by actively encouraging increased female participation in the cybersecurity field and supporting mid-career professionals who are looking to transition into cybersecurity roles.[16] By tapping into previously underrepresented groups and providing pathways for career changes, Thailand aims to alleviate the skills shortage and bring diverse perspectives to the cybersecurity workforce.

7. Impact of Geopolitical Events on Thailand's Cybersecurity Posture

Thailand's cybersecurity landscape is significantly influenced by the complex interplay of regional and global geopolitical events. Situated in a geostrategically important region, Thailand must navigate the delicate balance of cooperation and competition among major global powers, which has direct implications for its cybersecurity strategies and partnerships.[14] The nation's approach to cybersecurity is inherently shaped by these geopolitical realities, requiring careful consideration of its relationships with various international actors.

China's Digital Silk Road Initiative, a significant geopolitical undertaking, has led to an increased reliance by Thailand on Chinese digital infrastructure, particularly in areas such as 5G, artificial intelligence, and broader digital infrastructure development.[16] While this initiative offers opportunities for technological advancement and economic growth, it also raises concerns regarding data sovereignty and potential cybersecurity risks associated with this increased dependence on infrastructure from a specific geopolitical entity. This necessitates careful risk assessment and the implementation of robust mitigation strategies to safeguard Thailand's digital sovereignty and overall security.

In response to these geopolitical dynamics, Thailand is strategically pursuing a policy of diversification in its international collaborations. The nation is actively working with partners such as the European Union, Japan, and various regional allies to strengthen its cyber resilience while striving to maintain its strategic autonomy.[16] This diversification strategy aims to reduce the risks associated with over-reliance on any single geopolitical partner and to enhance Thailand's overall cybersecurity capabilities by leveraging a broader range of international expertise and best practices.

The presence of state-linked hacking groups, particularly those associated with China, operating within Southeast Asia, including Thailand, further underscores the geopolitical dimension of the cybersecurity threats facing the nation.[14] These state-sponsored threat actors often possess significant resources and advanced capabilities, potentially targeting government entities, critical infrastructure, and organizations holding sensitive information that could be of strategic interest to these actors' respective nations. This necessitates that Thailand develops enhanced threat intelligence capabilities and robust defensive strategies to effectively counter these sophisticated adversaries.

Regional geopolitical tensions, such as those in the South China Sea, and the broader rise of China as a major geostrategic power in Asia, can also indirectly escalate the risk of cyberattacks targeting Thailand.[14] In the current global landscape, cyber operations are increasingly being employed as tools in geopolitical competition, and heightened tensions in the region could translate into an increased risk of cyberattacks targeting Thailand's critical infrastructure, government networks, and other strategic assets.

On a global scale, the World Economic Forum's Global Risks Report 2025 has identified cyber warfare as a significant global risk.[18] This recognition at the international level highlights the growing importance of cybersecurity in the context of international relations and the potential for cyber conflicts to have far-reaching consequences for national security and stability. Furthermore, a significant majority (86%) of business leaders believe that global geopolitical instability is likely to lead to a catastrophic cyber event within the next two years.[27] This widespread concern among business leaders underscores the potential for significant cyber incidents, potentially with geopolitical underpinnings, to disrupt businesses and critical infrastructure in Thailand, emphasizing the critical need for enhanced cyber resilience and preparedness across all sectors.

8. Future Outlook and Predictions for Thailand's Cybersecurity

Looking ahead to 2025 and beyond, the cybersecurity landscape in Thailand is expected to become increasingly complex and challenging. The wider adoption of emerging technologies such as artificial intelligence, the Internet of Things, and cloud computing will continue to drive digital transformation across Thailand. However, this increasing interconnectedness and reliance on advanced technologies will also lead to a more diverse and sophisticated threat environment.[12] Organizations in Thailand will need to anticipate and prepare for a new wave of cyber threats that leverage these very technologies.

Specific types of cyberattacks, such as ransomware and supply chain attacks, are predicted to become even more serious concerns for Thai organizations in 2025.[12] The potential for significant financial and operational damage from ransomware, coupled with the widespread impact that can result from compromising vulnerabilities within supply chains, necessitates a strong focus on proactive prevention strategies. This includes implementing robust data backup and recovery mechanisms, strengthening endpoint security measures, and conducting thorough risk assessments of third-party vendors and partners.

The proliferation of deepfake technology is also expected to go mainstream in the Asia-Pacific region, including Thailand, in 2025.[8] This poses a significant threat for social engineering attacks, as the ability to create highly realistic fake videos and audio can make phishing and other deceptive tactics even more convincing and difficult to detect. Organizations in Thailand will need to enhance their user awareness training programs to educate employees about the risks of deepfakes and implement advanced authentication methods to mitigate the potential for successful social engineering attacks.

While the threat posed by quantum computing to current encryption methods is not yet an immediate concern, nation-state-backed threat actors are anticipated to intensify their "harvest now, decrypt later" tactics in 2025.[8] These actors may target highly classified data in Thailand with the long-term intent of decrypting it once quantum computing technology becomes sufficiently advanced. This long-term risk underscores the importance for government agencies and organizations handling highly sensitive information to begin exploring and transitioning to post-quantum cryptography solutions to ensure the security of their data in the future.

On the defensive side, technological advancements are also expected to play a crucial role in shaping Thailand's cybersecurity posture. Artificial intelligence is predicted to become central to cybersecurity

strategies in 2025, with organizations increasingly leveraging AI-powered tools and techniques to proactively mitigate risks and enhance their overall security posture.[8] By 2025, it is anticipated that a significant majority (90%) of cybersecurity tools will incorporate AI in some form.[2] This widespread integration of AI into security solutions highlights its transformative impact on the cybersecurity landscape, enabling more intelligent and adaptive threat detection, automated incident response, and proactive risk management capabilities for organizations in Thailand.

Market trends within the Thai cybersecurity sector also point towards continued growth in end-user spending on information security throughout 2025.[3] This sustained increase in investment reflects the ongoing recognition by organizations in Thailand of the critical importance of cybersecurity in protecting their digital assets and mitigating the ever-evolving range of cyber risks. Furthermore, the trend of organizations seeking to simplify their security operations by reducing the number of disparate cybersecurity tools they use and shifting towards more unified security platforms is expected to continue in 2025.[8] This drive for platform consolidation will likely fuel the adoption of integrated security solutions such as Extended Detection and Response (XDR) that offer comprehensive visibility and coordinated response capabilities across various security layers.

9. Notable Recent Cybersecurity Incidents and Breaches in Thailand

Recent years have seen a concerning trend of increasing cyberattacks targeting Thailand, highlighting the nation's vulnerability in the digital realm. Statistics indicate that cyberattacks in Thailand are occurring at a rate 70% higher than the global average.[9] This alarming statistic underscores the elevated cybersecurity risk faced by organizations operating within the country, suggesting that Thailand has become a significant target for cybercriminals, possibly due to a combination of factors including its rapid digital expansion and potentially varying levels of cybersecurity maturity across different sectors. The sheer volume of web threats detected in Thailand further emphasizes this point, with over 28,000 incidents blocked daily in 2024.[28] This constant barrage of malicious activity necessitates the implementation of robust and continuously updated security measures to effectively filter and block these numerous threats at various levels, including network, endpoint, and user. Moreover, Thai servers experienced a dramatic surge in cyberattacks in 2024, with the number of incidents increasing by a staggering 125.91% compared to 2023.[29] This significant rise in attacks targeting servers could be linked to the rapid expansion of data centers and cloud services within Thailand, making these critical infrastructure components attractive targets for attackers seeking to compromise large volumes of data or disrupt essential online services.

Several notable cybersecurity incidents and breaches have occurred in Thailand recently, illustrating the diverse range and potential impact of cyber threats. In early 2025, the cryptocurrency exchange Bybit reportedly suffered a massive $1.5 billion hack, with suspicion falling on the notorious North Korea-linked Lazarus Group.[29] This incident represents the largest cryptocurrency hack in history and underscores the significant financial risks associated with cyberattacks targeting digital asset platforms in Thailand. The involvement of a sophisticated state-sponsored group highlights the advanced nature of threats targeting this sector. Over the past two years (aligning with the 2024-2025 timeframe), Thai bank customers have collectively lost more than 60 billion baht to online financial fraud.[9] This staggering figure underscores the significant impact of online scams and fraudulent activities on individuals in Thailand, emphasizing the urgent need for stronger security measures within the banking sector and increased public awareness

campaigns to educate citizens on how to avoid becoming victims of financial cybercrime. The 2024 ThaiCERT report documented 1,827 cases of cyberattacks affecting Thailand, with the most common types of incidents including fake websites and URLs used for phishing, data theft aimed at exfiltrating sensitive information, and attacks designed to cause disruption of online services.[12] This data provides a snapshot of the prevailing cyber threats facing Thailand and can help organizations understand the most frequent attack vectors to better prioritize their security efforts.

The following table lists some notable cybersecurity incidents in Thailand for 2024-2025:

Date (Approx.)	Type of Incident	Affected Entity/Sector	Impact	Suspected Actor(s)
Early 2025	Cryptocurrency Hack	Bybit (Exchange)	$1.5 billion worth of crypto assets stolen	Lazarus Group
2022-2024	Online Financial Fraud	Thai Bank Customers	>60 billion baht lost	Cybercriminals
2024	Various Cyberattacks	Public & Private Sectors	1,827 cases reported: Fake websites, Data Theft, Service Disruption	Various

This table provides concrete examples of the cybersecurity challenges facing Thailand, illustrating the real-world consequences of cyberattacks across different sectors.

10. Conclusion and Strategic Recommendations

The cybersecurity landscape in Thailand for 2024-2025 presents a dynamic and challenging environment. The market is experiencing significant growth, driven by rapid digitalization and an increasing awareness of cyber risks. However, this growth is accompanied by an evolving threat landscape characterized by prevalent phishing attacks, persistent malware threats, a rise in data trafficking, and the emergence of sophisticated AI-powered cyber intrusions.

The Thai government has established a foundational regulatory framework and is actively pursuing various initiatives to strengthen the nation's cyber defenses and address the critical cybersecurity skills gap. The adoption of advanced security solutions like zero-trust architecture and XDR is gaining traction, although widespread and mature implementation still requires further effort. Geopolitical factors continue to exert a notable influence on Thailand's cybersecurity posture, necessitating a balanced approach to international collaborations. Recent years have witnessed a concerning surge in cyberattacks targeting Thailand, resulting in significant financial losses and operational disruptions. By embracing a collaborative and proactive stance, Thailand can effectively address the evolving cybersecurity challenges and build a more secure and resilient digital ecosystem for the future.

11. Strategic Recommendations

To navigate this complex landscape and ensure a secure digital future, a collaborative and proactive approach is essential for all stakeholders in Thailand.

For Businesses

- Prioritize investments in advanced security solutions, including AI-powered tools, XDR, and Zero Trust Architecture, to enhance threat detection, response, and prevention capabilities.
- Implement continuous user awareness training programs to mitigate the persistent threat of phishing and social engineering attacks.
- Develop robust incident response plans to effectively manage and recover from cyber incidents.
- Strengthen supply chain security to address vulnerabilities in third-party relationships.
- Ensure compliance with relevant regulations such as the PDPA and the Cybersecurity Act.

For Government Agencies

- Continue efforts to strengthen the regulatory framework, adapting it to address emerging threats and technological advancements.
- Sustain investment in cybersecurity education and training programs to address the significant skills gap within the public sector and across the nation.
- Enhance collaboration with international partners for threat intelligence sharing and capacity building to bolster Thailand's cyber resilience.
- Raise public awareness about evolving cyber threats and promote safe online practices.

For Cybersecurity Professionals

- Remain committed to continuous learning and professional development.
- Focus on acquiring in-demand skills in areas such as cloud security, AI-driven security, and incident response.
- Actively participate in community efforts and knowledge sharing initiatives to enhance Thailand's overall cybersecurity posture.

WORKS CITED

1. Thailand Cyber Security Industry Report | Market Analysis, Size & Overview, accessed March 31, 2025, https://www.mordorintelligence.com/industry-reports/thailand-cybersecurity-market
2. Thailand Cybersecurity Job Market: Trends and Growth Areas for 2025, accessed March 31, 2025, https://www.nucamp.co/blog/coding-bootcamp-thailand-tha-thailand-cybersecurity-job-market-trends-and-growth-areas-for-2025
3. Global information security spending to grow 15% in 2025, accessed March 31, 2025, https://www.nationthailand.com/blogs/business/tech/40041487
4. Thailand IT And Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030) - GII Research, accessed March 31, 2025, https://www.giiresearch.com/report/moi1690910-thailand-it-security-market-share-analysis.html
5. Cyber Security Summit | Thailand 2025 - Exito Media Concepts, accessed March 31, 2025, https://exito-e.com/cybersecuritysummit/thailand/
6. Thailand Cybersecurity Market Report- Q4 2024 - ReportLinker, accessed March 31, 2025, https://www.reportlinker.com/dlp/e629a924653bab053ab138e7f476f5ad
7. Rising Tide of Cyber Attacks in Thailand 2024: A Surge in Sensitive ..., accessed March 31, 2025, https://zerodarkweb.com/rising-tide-of-cyber-attacks-in-thailand-2024-a-surge-in-sensitive-personal-data-trafficking-on-the-dark-web/
8. Asia Pacific cybersecurity predictions: Trends for 2025 and beyond - Nation Thailand, accessed March 31, 2025, https://www.nationthailand.com/blogs/news/general/40044375
9. Thailand grapples with a cybersecurity crisis as attacks soar 70% higher than the global average, accessed March 31, 2025, https://www.thailand-business-news.com/crime/196696-thailand-grapples-with-a-cybersecurity-crisis-as-attacks-soar-70-higher-than-the-global-average
10. Cyber-attack surge plunges Thailand into security crisis - Bangkok Post, accessed March 31, 2025, https://www.bangkokpost.com/business/general/2963743/cyber-attack-surge-plunges-thailand-into-security-crisis
11. AI and Cybersecurity Trends for 2025 - PKF Thailand, accessed March 31, 2025, https://www.pkfthailand.asia/ai-and-cybersecurity-trends-for-2025/
12. Surge in cyberthreats predicted in 2025 - Bangkok Post, accessed March 31, 2025, https://www.bangkokpost.com/business/general/2927346/tkc-predicts-surge-in-cyberthreats-in-2025
13. Cybersecurity threatscape in Southeast Asia - Positive Technologies, accessed March 31, 2025, https://global.ptsecurity.com/analytics/cybersecurity-threatscape-in-southeast-asia
14. THE CHANGING CYBER THREAT LANDSCAPE SOUTHEAST ASIA - cyfirma, accessed March 31, 2025, https://www.cyfirma.com/research/the-changing-cyber-threat-landscape-southeast-asia/
15. ASEAN's Cyber Initiatives: A Select List | Strategic Technologies Blog - CSIS, accessed March 31, 2025, https://www.csis.org/blogs/strategic-technologies-blog/aseans-cyber-initiatives-select-list
16. Cybersecurity in Thailand: Balancing Progress, Geopolitical Influences, and the Need for Enhanced Readiness - FACTS Asia, accessed March 31, 2025, https://www.factsasia.org/blog/cybersecurity-in-thailand-balancing-progress-geopolitical-influences-and-the-need-for-enhanced-readiness
17. Thailand Cybersecurity Job Market: Trends and Growth Areas for 2024, accessed March 31, 2025, https://www.nucamp.co/blog/coding-bootcamp-thailand-tha-thailand-cybersecurity-job-market-trends-and-growth-areas-for-2024
18. NCSA ordered to step up preparations against cyber warfare - Nation Thailand, accessed March 31, 2025, https://www.nationthailand.com/news/policy/40047191
19. Zero Trust - Palo Alto Networks, accessed March 31, 2025, https://www.paloaltonetworks.com/zero-trust
20. Cisco's 2024 Cybersecurity Readiness Index - Thailand, accessed March 31, 2025, https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_TH.pdf
21. Extended Detection and Response (XDR) Global Markets 2024-2027: Leveraging New Capabilities to Expand Across Regions and Maturity Levels, Developing New Technology, Detections, and Intelligence - GlobeNewswire, accessed March 31, 2025, https://www.globenewswire.com/news-release/2025/02/26/3033119/28124/en/Extended-Detection-and-Response-XDR-Global-Markets-2024-2027-Leveraging-New-Capabilities-to-Expand-Across-Regions-and-Maturity-Levels-Developing-New-Technology-Detections-and-Intel.html
22. Extended Detection and Response (XDR) Global Market Forecasts 2024 & 2025-2027: AI Advancements, Third-party Integration, and a Proactive Approach to Security Fueling Opportunities - ResearchAndMarkets.com - Business Wire, accessed March 31, 2025, https://www.businesswire.com/news/home/20250303595398/en/Extended-Detection-and-Response-XDR-Global-Market-Forecasts-2024-2025-2027-AI-Advancements-Third-party-Integration-and-a-Proactive-Approach-to-Security-Fueling-Opportunities---ResearchAndMarkets.com

23. Extended Detection and Response Market Size, Trends - 2034 - Market Research Future, accessed March 31, 2025, https://www.marketresearchfuture.com/reports/extended-detection-response-market-12210
24. Thailand sees more than 28000 web threats per day - Bangkok Post, accessed March 31, 2025, https://www.bangkokpost.com/business/general/2974171/thailand-sees-more-than-28-000-web-threats-per-day
25. Cybersecurity Governance in Southeast Asia, accessed March 31, 2025, https://www.dcaf.ch/sites/default/files/publications/documents/Cybersecurity_Governance_in_Southeast_Asia_Thematic_Brief.pdf
26. THE CHANGING CYBER THREAT LANDSCAPE SOUTHEAST ASIA - cyfirma, accessed March 31, 2025, https://www.cyfirma.com/research/the-changing-cyber-threat-landscape-southeast-asia-2/
27. Cybersecurity Consulting Services & Strategies - Accenture, accessed March 31, 2025, https://www.accenture.com/us-en/services/cybersecurity
28. More than 28K web threats per day in Thailand, accessed March 31, 2025, https://www.nationthailand.com/business/tech/40046084
29. Historic crypto heist highlights Thailand's cybersecurity crisis - Nation Thailand, accessed March 31, 2025, https://www.nationthailand.com/business/tech/40046647
30. 5 Reasons to Implement Zero Trust & 5 Steps to Get You Started - Syteca, accessed March 31, 2025, https://www.syteca.com/en/blog/zero-trust-implementation