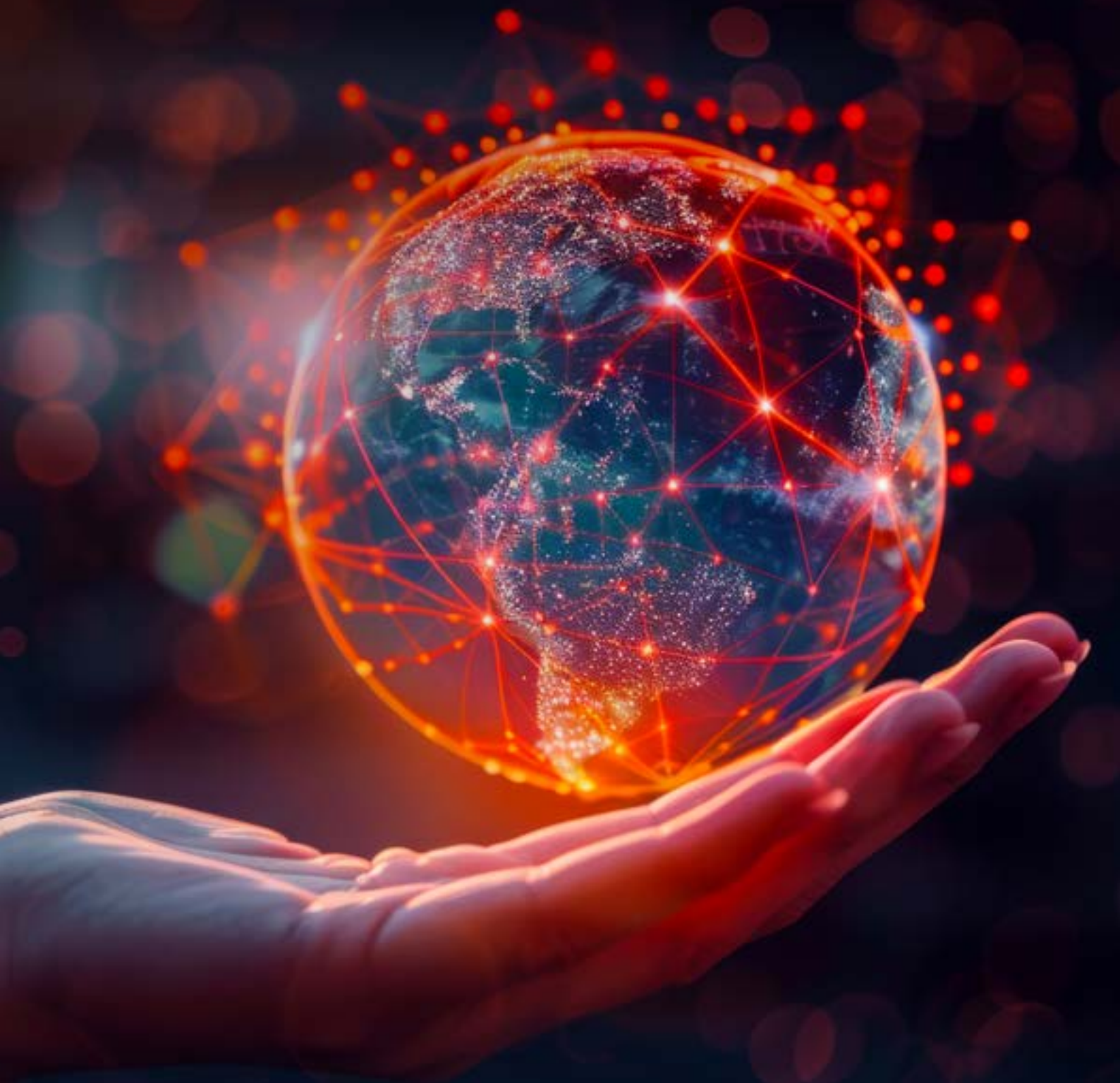
2024 Cybersecurity Awareness Month:

A Call to Action for a Secure World

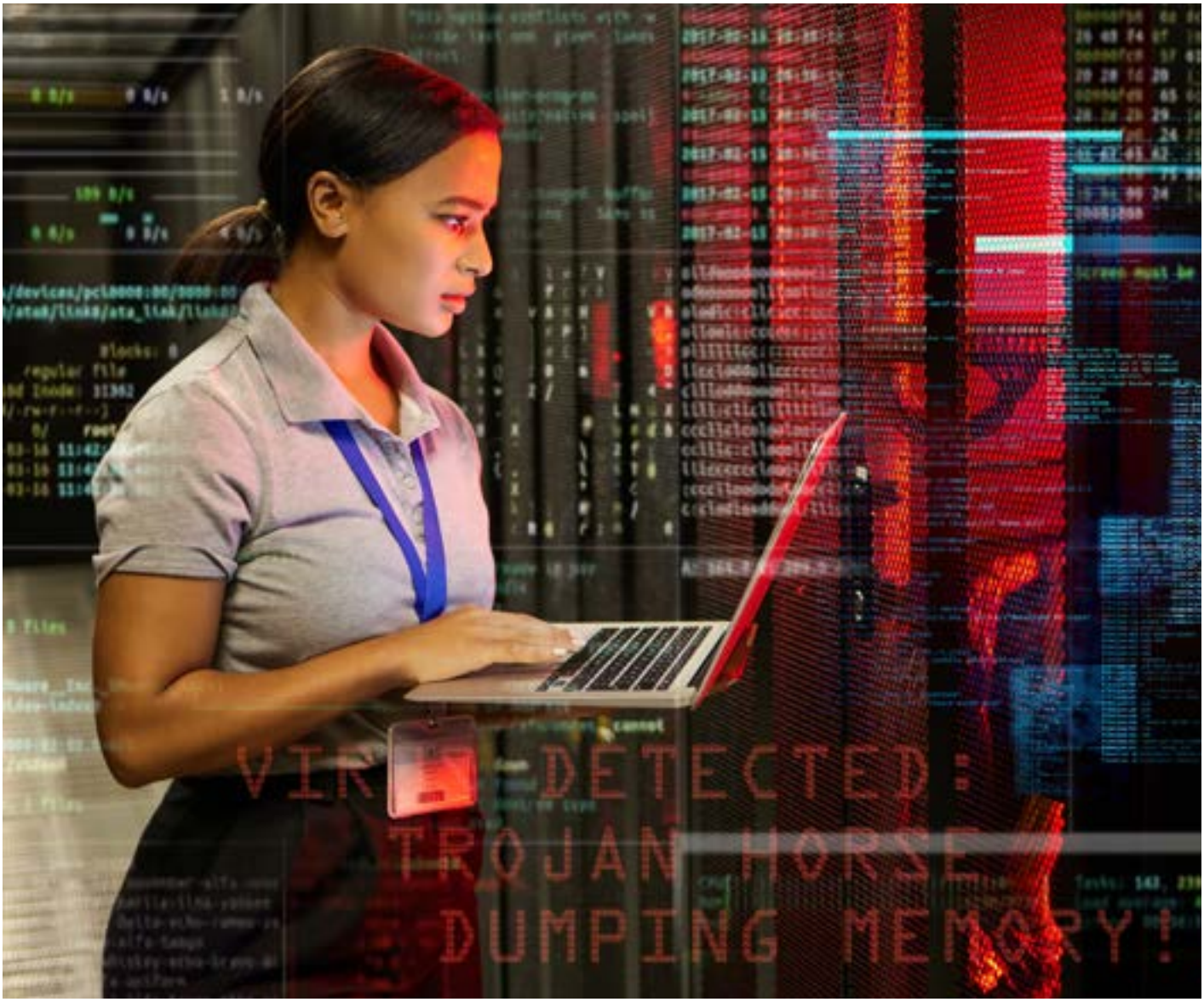


INTRODUCTION TO CYBERSECURITY AWARENESS MONTH

INTRODUCTION TO CYBERSECURITY AWARENESS MONTH

Cybersecurity Awareness Month is an annual initiative launched to educate individuals, businesses, and governments about the importance of cybersecurity and to encourage the adoption of sound cybersecurity practices. In 2024, the global theme is "Secure the World," emphasizing the collective responsibility to safeguard the digital ecosystem against increasing cyber threats. The month-long campaign aims to raise awareness, improve resilience, and create a safer digital world.

This whitepaper delves into the evolving global cybersecurity landscape, regional threat assessments, and key initiatives to address compliance and regulatory requirements. It highlights the growing need for collaboration between governments, enterprises, and individuals to ensure a secure and resilient cyber environment.



KEY FINDINGS

1

Rise in Ransomware Attacks Globally

A significant increase in ransomware attacks, particularly in critical infrastructure and healthcare, was observed globally in 2024. The Americas alone saw a 35% rise.

2

Supply Chain Vulnerabilities in Europe

Europe experienced a 20% rise in supply chain attacks, particularly affecting manufacturing and logistics, showing the vulnerability of interconnected systems.

3

Cybercrime Costs in ASEAN

The financial impact of cybercrime in the ASEAN region is projected to exceed $300 billion by the end of 2024.

4

Data Breaches in India

Nearly 1 billion records were compromised in India in 2024, exposing significant vulnerabilities in data protection.

5

Advanced Persistent Threats (APTs) in ANZ

The ANZ region saw an increase in sophisticated attacks like APTs, often targeting government institutions and critical infrastructure.

6

Phishing Dominates Attack Vectors

Phishing continues to dominate the cyber threat landscape, accounting for 41% of all cyber incidents in the Americas.

7

Increased Investment in Cybersecurity

Investment in cybersecurity across regions has seen a dramatic increase, with Europe and ASEAN leading with a 30% rise in budgets allocated to cybersecurity.

8

Workforce Shortage in Cybersecurity

Europe reported that 75% of organizations are experiencing a shortage of skilled cybersecurity professionals, a trend echoed in other regions.

9

Governance and Compliance Focus

Countries worldwide, especially in Europe and the Americas, are tightening regulatory frameworks, with GDPR and the NIS2 Directive being prominent examples.

10

Government Initiatives in Cybersecurity

Regional governments, such as those in the META region and ASEAN, are increasingly adopting advanced cybersecurity frameworks and regulations to improve national resilience against cyber threats.

CYBERSECURITY AWARENESS AND THE GLOBAL THREAT LANDSCAPE

Cybersecurity Awareness Month 2024 brings global attention to the rapidly evolving cyber threat landscape. As more regions adopt digital technologies, cybercriminals exploit vulnerabilities on a massive scale, leading to widespread data breaches, ransomware attacks, and advanced persistent threats (APTs).

The threat landscape continues to evolve, with cybercriminals using sophisticated methods to breach defenses. Phishing, ransomware, and supply chain attacks are just a few examples of the types of cyber threats that have emerged as major global concerns. As cyberattacks grow in frequency and impact, it is essential for businesses, individuals, and governments to understand the nature of these threats and prioritize cybersecurity. The 2024 theme, "Secure the World," serves as a call to action for all stakeholders to strengthen their defenses, ensure compliance with regulations, and foster a cybersecurity culture that prioritizes prevention, awareness, and resilience.

REGIONAL ANALYSIS

AMERICAS: AN INCREASE IN RANSOMWARE AND PHISHING

In 2024, the Americas have witnessed a substantial increase in ransomware attacks, particularly targeting critical sectors like healthcare and infrastructure.

- **Data Breaches:** Over 1,200 breaches have exposed nearly 600 million records.
- **Ransomware:** A 35% rise in ransomware incidents, with ransom demands growing exponentially.
- **Phishing:** 41% of all cyberattacks involved phishing, making it the most prevalent attack vector.
- **Investments:** Cybersecurity investments in the Americas increased by 25%, reflecting a focus on building robust security measures.

Governments and private institutions alike have responded to these threats by increasing their cybersecurity budgets, implementing advanced threat detection technologies, and prioritizing incident response capabilities.

EUROPE: SUPPLY CHAIN ATTACKS AND REGULATORY EMPHASIS

Europe's cybersecurity posture in 2024 has been characterized by regulatory stringency and the growing impact of supply chain attacks.

- **Data Breaches:** GDPR penalties have increased by 50%, with more stringent enforcement on data protection violations.
- **Supply Chain Attacks:** A 20% increase in supply chain-related cyberattacks, especially in manufacturing and logistics sectors.
- **Workforce Shortage:** 75% of organizations in Europe report a shortage of skilled cybersecurity personnel.
- **Investments**: Companies have increased their cybersecurity budgets by 30% in response to both regulatory pressures and rising threats.

Europe's regulatory environment is one of the strictest globally, with enhancements to GDPR and the introduction of NIS2 focusing on protecting digital infrastructure.

REGIONAL ANALYSIS

ASEAN: ACCELERATING DIGITALIZATION AMID RISING CYBERCRIME COSTS

ASEAN countries continue to grapple with rising cybercrime costs, which are projected to exceed $300 billion by the end of 2024.

- **Cybercrime Costs:** Up from $240 billion in 2023, cybercrime costs continue to burden businesses and governments alike.
- **Small and Medium Enterprises (SMEs):** SMEs remain particularly vulnerable, with a 40% increase in reported cyber incidents.
- **Government Initiatives:** Strategic frameworks are being implemented across the region to strengthen cybersecurity resilience.
- **Public Awareness:** A 15% rise in public awareness campaigns has improved basic cybersecurity hygiene across the population.

Governments in ASEAN are increasingly adopting comprehensive cybersecurity strategies aimed at protecting national infrastructures, SMEs, and individual citizens.

META (MIDDLE EAST, TURKEY, AND AFRICA): A REGION UNDER SIEGE

The META region continues to experience frequent and sophisticated cyberattacks, with financial and energy sectors being prime targets.

- **Cyber Attacks:** A 50% increase in cyberattacks, with ransomware incidents rising by 45%.
- **Threat Intelligence:** Organizations in META are increasingly adopting advanced threat intelligence solutions to combat sophisticated threats.
- **Investment:** A 22% increase in cybersecurity spending has been driven by regulatory requirements and the need for improved resilience.

Governments in META are enacting stronger cybersecurity laws and enhancing threat intelligence capabilities to stay ahead of cybercriminals.

REGIONAL ANALYSIS

INDIA: DATA BREACHES AND GOVERNMENT INITIATIVES

India faces unique cybersecurity challenges in 2024, with a surge in data breaches and phishing attacks.

- **Data Breaches:** Nearly 1 billion records were compromised in 2024, highlighting weaknesses in data protection.
- **Phishing:** Phishing and malware attacks remain the most prevalent threats, leading to a 30% increase in reported incidents.
- **Government Policies:** India's government has introduced new cybersecurity policies aimed at safeguarding critical information infrastructure and personal data.

India's strategic focus on cybersecurity is evident through its increased regulatory efforts and investment in national cybersecurity initiatives.

ANZ (AUSTRALIA AND NEW ZEALAND): FOCUS ON ADVANCED THREATS

Australia and New Zealand have taken a proactive stance on cybersecurity, with advanced persistent threats (APTs) becoming a prominent concern.

- **Advanced Threats:** An increase in sophisticated threats, including APTs and supply chain attacks.
- **Investment:** Cybersecurity budgets have risen by 28%, with 88% of CIOs prioritizing cybersecurity investments for 2025.
- **Data Breach Costs:** The average cost of a data breach in ANZ has risen by 15%, leading to more aggressive prevention measures.

ANZ's strategic focus on cybersecurity reflects a regional commitment to improving resilience against growing cyber threats.

COMPLIANCE AND GOVERNANCE: GLOBAL PERSPECTIVES

As cyber threats continue to evolve in complexity and scale, governments worldwide are responding by establishing more rigorous regulatory frameworks and enhancing governance protocols aimed at mitigating these risks. The need for a unified, global approach to cybersecurity governance is becoming increasingly evident as cybercriminals exploit cross-border vulnerabilities and target industries that lack robust protections. As a result, regions across the world are implementing laws, guidelines, and best practices to enforce compliance, reduce vulnerabilities, and strengthen cybersecurity resilience.

Key areas of focus in these regulations include mandatory breach notifications, stricter data privacy controls, and enhanced cybersecurity standards for critical infrastructures. In response to the rise in ransomware, phishing, and advanced persistent threats (APTs), many countries are pushing for increased transparency, with laws requiring rapid reporting of cyber incidents, as well as imposing hefty penalties for non-compliance. This proactive stance on cybersecurity governance reflects the understanding that cyber threats are not just a technological issue, but a governance, risk management, and compliance concern as well.

Beyond regulatory enforcement, global governments are also fostering public-private partnerships to address cybersecurity challenges. These collaborations enable the sharing of threat intelligence, promote innovation in cybersecurity solutions, and ensure a coordinated response to large-scale cyber incidents. Moreover, the evolving threat landscape requires a balance between security and privacy, with laws being updated to account for emerging technologies such as artificial intelligence (AI), the Internet of Things (IoT), and 5G, which introduce new risks but also offer opportunities for better cyber defense mechanisms.

The future of cybersecurity governance lies in agility and collaboration, as cyber threats will continue to evolve faster than the regulatory environment. Global harmonization of laws, the establishment of cross-border data protection agreements, and a stronger emphasis on cyber resilience will be crucial in shaping the future of cybersecurity governance.

COMPLIANCE AND GOVERNANCE: GLOBAL PERSPECTIVES

AMERICAS: STRENGTHENING CRITICAL INFRASTRUCTURE AND DATA PROTECTION

In the Americas, both North and South America are seeing significant regulatory enhancements in response to the growing cybersecurity threats.

United States

The United States has taken a particularly aggressive approach with the implementation of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). This law mandates that critical infrastructure operators report significant cyber incidents within 72 hours. The Act is aimed at improving the national response to cyberattacks on critical sectors such as energy, finance, and healthcare, which have become frequent targets of ransomware and state-sponsored attacks. By requiring rapid incident reporting, the U.S. government hopes to identify and mitigate threats faster, preventing widespread disruption.

Another major legislative effort is the Federal Data Protection Act, which introduces stricter guidelines for how data is stored, processed, and protected. The law imposes hefty penalties for data breaches and non-compliance, significantly raising the stakes for organizations that fail to adequately protect consumer data. The Act represents a shift towards holding businesses more accountable for cybersecurity lapses and is in line with the global trend of tightening data protection regulations.

Brazil

In Latin America, Brazil has updated its General Data Protection Law (LGPD) to impose more rigorous data security measures, particularly around data handling and breach response. These updates align Brazil's regulations more closely with global standards such as the European GDPR, reflecting the country's commitment to improving its cybersecurity posture. Brazil's enforcement of these new standards is particularly important as the country grapples with a rising number of cyber incidents targeting both public and private sectors.

COMPLIANCE AND GOVERNANCE: GLOBAL PERSPECTIVES

EUROPE: PIONEERING REGULATORY STANDARDS WITH GDPR AND NIS2

Europe has long been at the forefront of global cybersecurity regulation, and 2024 has seen further enhancements to its already stringent legal framework.

General Data Protection Regulation (GDPR) Enhancements

The GDPR remains a cornerstone of data protection law in Europe, and recent updates to this regulation reflect the evolving cyber threat landscape. One of the key areas addressed in these updates is the challenge posed by emerging technologies such as artificial intelligence (AI) and machine learning (ML). The GDPR now includes clearer guidelines on the use of AI in data processing, ensuring that privacy rights are maintained even as technology advances. The updates also tighten rules around cross-border data transfers, reflecting the need for greater control over how data is shared between regions, particularly with the rise of cloud computing and globalized digital services.

Network and Information Security Directive 2 (NIS2)

Europe has also introduced the NIS2 Directive, which implements stricter cybersecurity requirements for a broader range of digital services and critical infrastructure sectors. NIS2 extends the scope of cybersecurity regulation to more industries, including healthcare, energy, and transportation, emphasizing the need for robust incident reporting mechanisms and enhanced cybersecurity standards. The directive is a direct response to the increase in ransomware attacks and supply chain vulnerabilities across Europe, aiming to boost the overall security posture of the continent.

Digital Services Act (DSA)

The Digital Services Act imposes new obligations on online platforms to combat illegal content and protect user data more effectively. This Act focuses on reducing the spread of misinformation, ensuring transparency in digital advertising, and safeguarding user privacy. For large tech companies operating in Europe, the DSA introduces a more comprehensive framework for data handling, content moderation, and platform accountability.

COMPLIANCE AND GOVERNANCE: GLOBAL PERSPECTIVES

ASEAN: RISING CYBERCRIME COSTS AND STRATEGIC FRAMEWORKS

The Association of Southeast Asian Nations (ASEAN) has witnessed a dramatic increase in cybercrime, with costs projected to exceed $300 billion by the end of 2024. In response, several ASEAN countries have ramped up their regulatory frameworks to bolster cybersecurity.

Singapore: Cybersecurity Act 2024

Singapore's Cybersecurity Act 2024 is a landmark piece of legislation that mandates critical infrastructure operators to adopt stringent cybersecurity measures and report significant incidents promptly. The Act is designed to protect vital sectors such as telecommunications, healthcare, and finance from cyber threats, and it imposes severe penalties for non-compliance. Singapore has also enhanced its data protection laws under the Personal Data Protection Act (PDPA), which now includes stricter breach notification timelines and higher penalties for non-compliance.

Malaysia: National Cyber Security Strategy 2024

Malaysia's National Cyber Security Strategy 2024 lays down comprehensive guidelines aimed at fortifying the country's defenses against cyber threats. This strategy covers both public and private sectors, focusing on data protection, incident response, and building national resilience. The plan emphasizes the need for stronger collaboration between the government and businesses to share threat intelligence and bolster cybersecurity capabilities.

COMPLIANCE AND GOVERNANCE: GLOBAL PERSPECTIVES

META (MIDDLE EAST, TURKEY, AND AFRICA): ADVANCED THREATS AND REGULATORY REINFORCEMENT

The META region continues to face an escalating number of sophisticated cyberattacks, particularly targeting sectors like finance, energy, and government infrastructure.

United Arab Emirates: Cybercrime Law 2024

The Cybercrime Law 2024 in the UAE introduces stringent penalties for cyber offenses and expands the scope of regulations related to data protection. The law targets both domestic and international actors involved in cyberattacks on UAE's critical infrastructure. By enhancing these penalties, the UAE aims to deter cybercriminals from targeting its rapidly expanding digital economy.

Saudi Arabia: National Cybersecurity Strategy

Saudi Arabia has taken a comprehensive approach to cybersecurity with its National Cybersecurity Strategy, which focuses on securing critical infrastructure and mitigating risks posed by digital transformation. The strategy promotes the adoption of advanced cybersecurity technologies, such as AI and machine learning, to protect against increasingly sophisticated cyber threats.

COMPLIANCE AND GOVERNANCE: GLOBAL PERSPECTIVES

INDIA: DATA PROTECTION AND PUBLIC-PRIVATE COLLABORATION

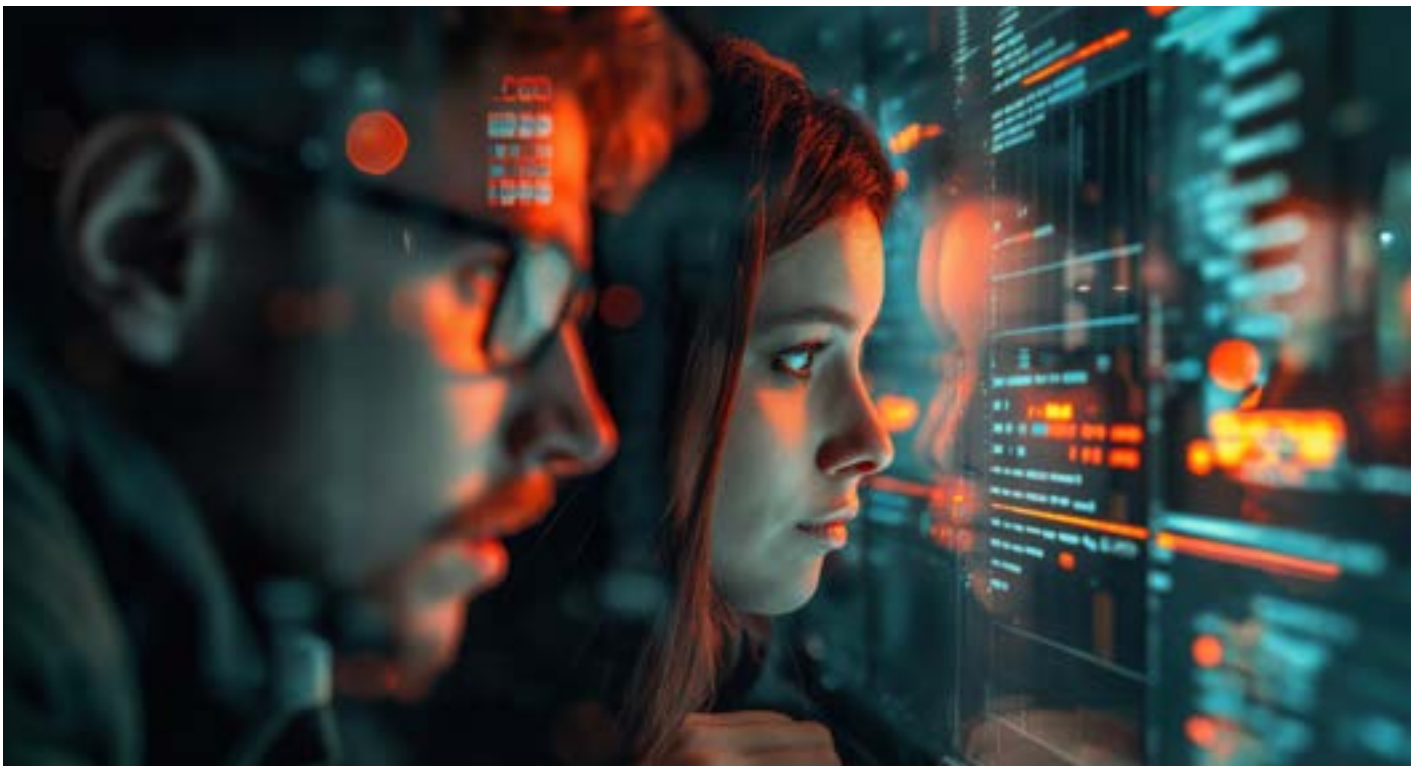
India's fast-growing digital economy has made it a prime target for cybercriminals, prompting the government to implement more robust cybersecurity regulations.

Digital Personal Data Protection Bill 2022

The Digital Personal Data Protection Bill 2022 sets comprehensive data protection requirements, covering everything from how data is collected and stored to how breaches are reported. The bill introduces severe penalties for non-compliance and establishes the Data Protection Authority (DPA), which is tasked with ensuring compliance across industries. This regulatory framework is crucial for protecting the personal data of over a billion people in India, particularly as the country experiences rapid digital growth.

National Cybersecurity Policy 2024

India's National Cybersecurity Policy 2024 emphasizes protecting critical infrastructure, enhancing threat intelligence sharing, and promoting collaboration between the public and private sectors. The policy outlines the need for stronger partnerships to address the evolving cyber threat landscape, with a particular focus on sectors like banking, telecommunications, and healthcare.



COMPLIANCE AND GOVERNANCE: GLOBAL PERSPECTIVES

ANZ (AUSTRALIA AND NEW ZEALAND): CRITICAL INFRASTRUCTURE AND DATA PROTECTION

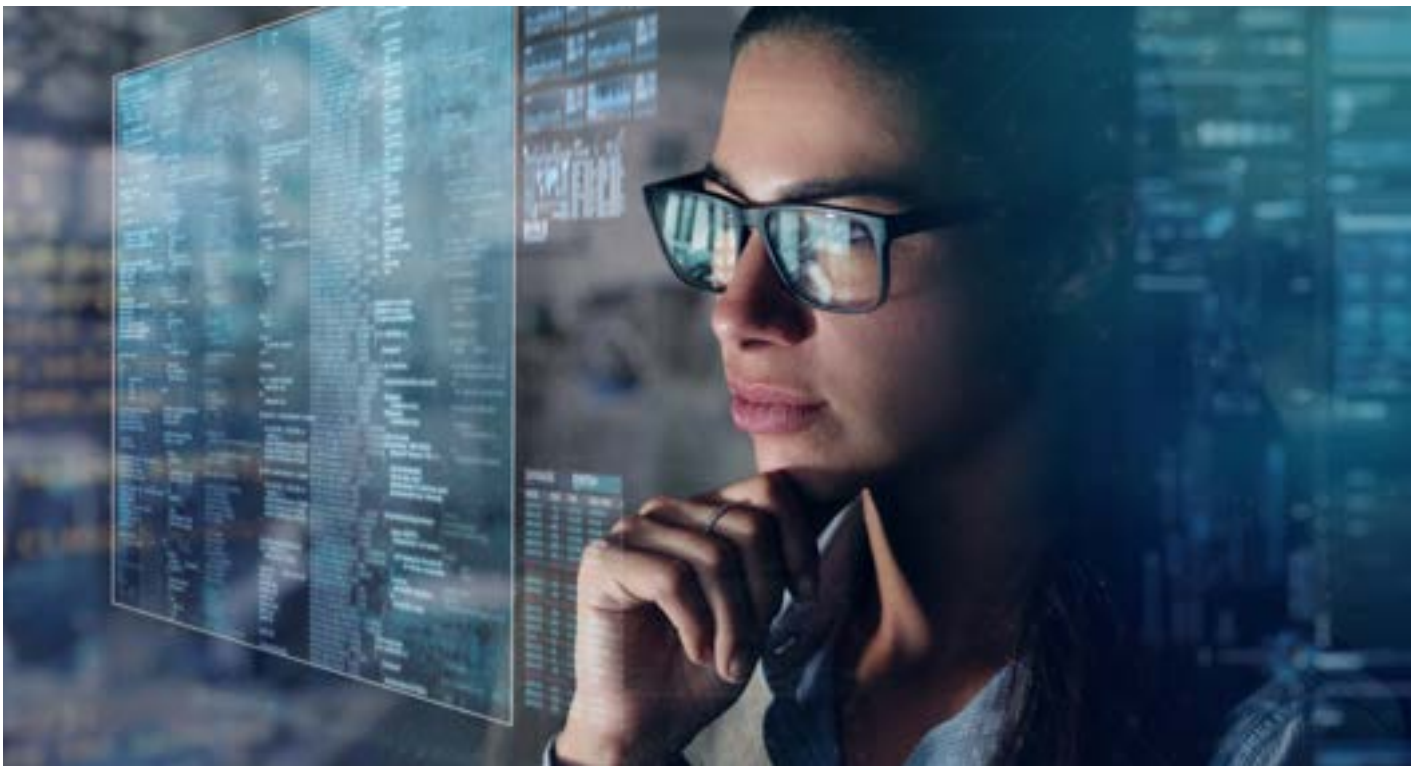
Australia and New Zealand have both introduced stringent regulations to address the growing number of cyber incidents targeting critical infrastructure and sensitive data.

Australia: Critical Infrastructure and Systems of National Significance Act 2024

Australia's Critical Infrastructure and Systems of National Significance Act 2024 mandates that operators of critical infrastructure adopt robust cybersecurity measures and report cyber incidents within specific timelines. The Act aims to protect vital sectors such as energy, healthcare, and transportation from both domestic and foreign cyber threats, reflecting Australia's focus on national security.

New Zealand: Privacy Act 2020 Amendments

New Zealand has made significant updates to its Privacy Act 2020, extending the scope of data breach notifications and introducing stricter cross-border data transfer regulations. The amendments also impose higher penalties for non-compliance, reflecting the country's commitment to safeguarding personal data in an increasingly interconnected digital environment.



THE FUTURE OF CYBERSECURITY

As the world continues to embrace digital transformation, the importance of cybersecurity becomes even more pronounced. The 2024 Cybersecurity Awareness Month theme, "Secure the World," serves as a powerful reminder of the collective responsibility to safeguard the digital ecosystem. From the Americas to ANZ, the global threat landscape is evolving rapidly, with cybercriminals employing sophisticated techniques to exploit vulnerabilities and cause widespread damage.

Ransomware, phishing, supply chain attacks, and advanced persistent threats have emerged as major global concerns, impacting individuals, businesses, and governments alike. The financial implications of these attacks are staggering, with costs projected to reach hundreds of billions of dollars across regions. Data breaches are becoming increasingly frequent, exposing sensitive information and jeopardizing privacy.

However, amid these challenges, there is also a growing recognition of the importance of cybersecurity. Governments worldwide are enacting stricter regulations and enhancing governance protocols to mitigate risks and improve resilience. From the United States' CIRCIA to Europe's NIS2 Directive, and from India's Digital Personal Data Protection Bill to Australia's Critical Infrastructure Act, these regulatory initiatives aim to create a safer digital world by enforcing compliance, promoting transparency, and holding organizations accountable for cybersecurity lapses.

In addition to regulatory efforts, public-private partnerships are fostering collaboration, innovation, and a coordinated response to cyber threats. The sharing of threat intelligence, the development of advanced security technologies, and the promotion of cybersecurity awareness are all critical components of this collaborative approach.

As we look to the future, it is clear that cybersecurity will continue to be a top priority for governments, businesses, and individuals around the world. The challenges are complex and multifaceted, but the opportunities for collaboration, innovation, and resilience are also immense. By prioritizing cybersecurity, investing in advanced technologies, and fostering a culture of awareness and prevention, we can secure the world against the ever-evolving cyber threats and ensure a safe and prosperous digital future for all.

Industry Recognition

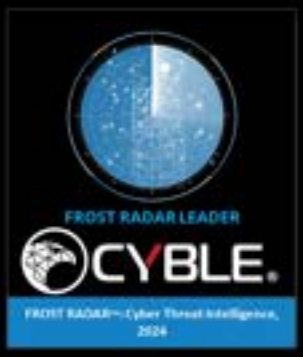
Gartner

Cyble Named a Sample Vendor in Three Gartner® Hype Cycles for Managed IT Services, 2024, Cyber Risk Management, 2024 and Security Operations, 2024

FORRESTER®

Cyble Recognized in Forrester's Attack Surface Management Solutions Landscape Q2-2024 Report

FROST & SULLIVAN



Cyble Named Leader in Frost Radar™ Cyber Threat Intelligence 2024

Gartner Peer Insights.

4.6/5

Ranked among top 5 cyber threat intelligence providers

Named a leader in the G2 Grid for Dark Web Monitoring

Named Editor's Choice for Threat Intelligence by Cyber Defense Magazine

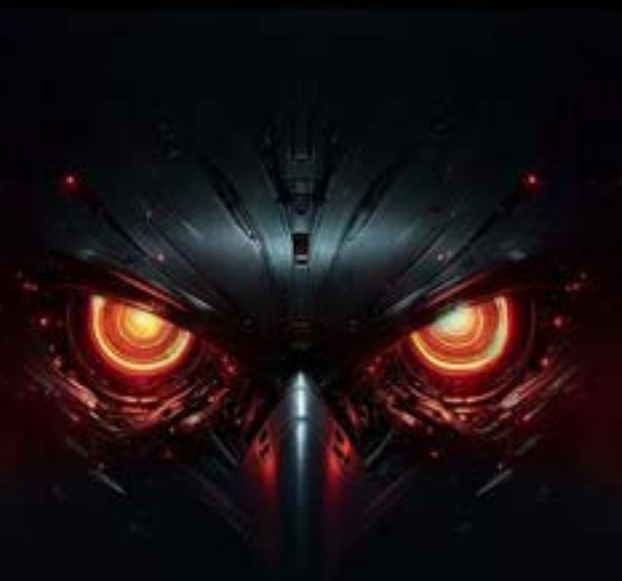
Earned nine awards at the Global InfoSec Awards during RSA

Ranked in Y Combinator's Top 100 AI Startups for 2024

Recognized as one of America's Best Startup Employers by Forbes

CYBLE.

Cyble provides one of the fastest and most comprehensive coverages across adversaries, infrastructure, exposure, weaknesses, and targets by leveraging cutting-edge AI technology and real-time threat intelligence and detection. Through advanced data analysis, expert insights, and automated processes, Cyble facilitates swift detection, prioritization, and remediation of security threats, and enables governments and enterprises to protect their citizens and infrastructure by delivering crucial intelligence promptly. Headquartered in Atlanta, GA, and with employees across 12 countries, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com



11175 Cicero Drive Suite, 100 Alpharetta GA 30022, US. | contact@cyble.com | +1 888 673 2067