CYBLE®

REPORT

From Projection to Proof: **Cyble's 2024 Forecast Validated**

From ICS Exploits to AI-Enhanced Attacks, Cyble's Cybersecurity Predictions 2024 Hits Bull's Eye!

In early January, this year, Cyble released its highly anticipated Annual Threat Landscape Report, that provided an in-depth analysis of the year gone-by and a peep into the emerging threats and trends in cybersecurity for the year ahead.

With a foundation built on AI-powered advanced threat intelligence, rigorous research, and years of experience in the cybersecurity domain, Cyble's Annual Treat Landscape report not only highlighted key vulnerabilities but also predicted how these would manifest in the coming year.

These predictions were not mere conjectures but a roadmap, grounded in real-world data and insights, that warned of specific vulnerabilities, evolving tactics, and potential ramifications.

As the year 2024 unfolded, Cyble's foresight proved to hit the bull's eye! The landscape of cybersecurity was shaped by the very challenges and incidents that Cyble gave early warnings of. Ranging from the escalation of Industrial Control System (ICS) exploits to the pervasive impact of AI-enhanced social engineering attacks, each prediction was a testament to Cyble's unparalleled ability to anticipate and navigate the complexities of the ever-evolving digital threat ecosystem.

This retrospective examines how Cyble's predictions materialized, the real-world incidents that validated them, and the broader implications for organizations and industries worldwide.

Prediction 1: Surge in ICS-Specific Exploits

TRUE

PROOF

Industrial Control Systems (ICS) emerged as a prime target for cyberattacks in 2024. Cyble not only forecasted targeted attacks on this sector but also the gauged the possibility of attacks through vulnerability exploitation within critical infrastructure. This came true as operational and economic ramifications of these attacks were far-reaching, as several high-profile incidents demonstrated:

- **FrostyGoop Malware:** In April 2024, the discovery of FrostyGoop showcased the sophisticated nature of modern ICS threats. This malware, the ninth of its kind targeting ICS, exploited the Modbus protocol to infiltrate operational technology environments. By directly interacting with critical infrastructure systems, FrostyGoop posed a substantial risk to industrial operations, including energy grids and manufacturing plants.

  Read: Russia-Linked FrostyGoop Malware Threatens Industrial Control Systems Worldwide

- **Active Exploitation of ICS Devices:** By September 2024, attackers had ramped up efforts to exploit internet-accessible ICS devices. Unsophisticated yet effective methods such as brute force attacks and default credential exploits were widely used. Notably, the Water and Wastewater Systems sector was a primary target, highlighting the dire need for improved cybersecurity measures in utilities.

  Read: Drinking Water Systems for 27 Million Americans Have High-Risk Security Vulnerabilities

- **Anticipated Vehicle Control System Attacks:** The report also foresaw potential attacks on fleets of vehicles with identical control systems. These predictions materialized as attackers leveraged telemetry-gathering equipment to compromise connected vehicles, broadening the scope of ICS vulnerabilities beyond traditional industrial environments. The U.S. proposed stringent measures including bans to counter this threat.

  Read: Biden Administration Proposes Ban on Chinese and Russian Vehicle Connectivity Systems

Additionally, multiple ICS sector-specific vulnerabilities were exploited, including:

- **CVE-2024-33789:** A command injection flaw in Linksys E5600 routers enabled remote attackers to execute arbitrary commands.
- **CVE-2024-7587:** Incorrect default permission in ICONICS Suite and Mitsubishi Electric MC Works64 allowed unauthorized system modifications.
- **CVE-2024-7113:** Resource allocation issues in Aveva products led to denial-of-service attacks.

Predictions 2: Spread of Disinformation and Fake News

TRUE

PROOF

The proliferation of disinformation and fake news, as predicted by Cyble, reached unprecedented levels in 2024 as more than half of the world's population voted in probably the biggest and defining election year we have ever witnessed. This phenomenon significantly impacted geopolitical stability, public trust, and the broader information ecosystem.

- **Russian Election Interference:** Following the 2024 U.S. elections, coordinated disinformation campaigns aimed to undermine public support for Ukraine. Doctored videos portraying Ukrainian soldiers negatively were disseminated widely, fueling misinformation and eroding trust in foreign policy initiatives of the state.

  Read: Did Russian Disinformation Change the U.S. Election Outcome?

- **State-Sponsored Campaigns:** Suspected state-sponsored actors exploited platforms like Twitter and Telegram to spread disinformation globally, with a specific focus on Western Europe and North America. These campaigns shaped public opinion, heightened tensions, and propagated false narratives about the Russia-Ukraine conflict.

  Read: OpenAI Exposes AI-Powered State Actors in Global Influence Operations

- **AI-Driven Misinformation:** The Australian Senate's inquiry into AI-driven misinformation highlighted concerns about the misuse of AI to create bioweapons and spread false information. This led to calls for stricter regulations to mitigate AI-related risks.

  Read: Senate AI Inquiry Worried at Threat to Australian Democracy

Also, the World Economic Forum's 2024 Global Risks Report identified misinformation and disinformation as critical global risks.

Prediction 3: AI-Enhanced Social Engineering Attacks

TRUE

PROOF

The integration of artificial intelligence into cyberattacks represented a significant evolution in threat sophistication. Cyble's prediction about AI-enhanced social engineering attacks was borne out by numerous high-profile incidents:

- **Deepfake Scams in Southeast Asia:** One of the most notable incidents occurred in Hong Kong, where a deepfake video call impersonating a company's CEO and colleagues led to millions in losses. This incident showcased the growing capability of AI to deceive and exploit human trust.

  Read: Deepfaked! Multinational Company in Hong Kong Falls Victim to $25 Million Deepfake Scam

- **Targeted Political Deception:** U.S. Senator Ben Cardin became a victim of an AI-driven deepfake operation. Attackers impersonated a former Ukrainian official to engage in sensitive political discussions, highlighting the political and security implications of AI-enhanced attacks.

  Read: 'Deepfake' Caller Poses as Ukrainian Official in Exchange With Key Senator

- **Hospitality Industry Scams:** AI-enabled scams targeting the hotel and travel industry surged in 2024. Attackers used AI-generated voices to mimic known professionals, tricking hotel staff into divulging sensitive financial information.

Read: Hotels and Travel Firms Battle AI Phone Scams

By leveraging AI, cybercriminals crafted highly personalized messages that bypassed traditional security measures, emphasizing the need for advanced detection tools and user education.

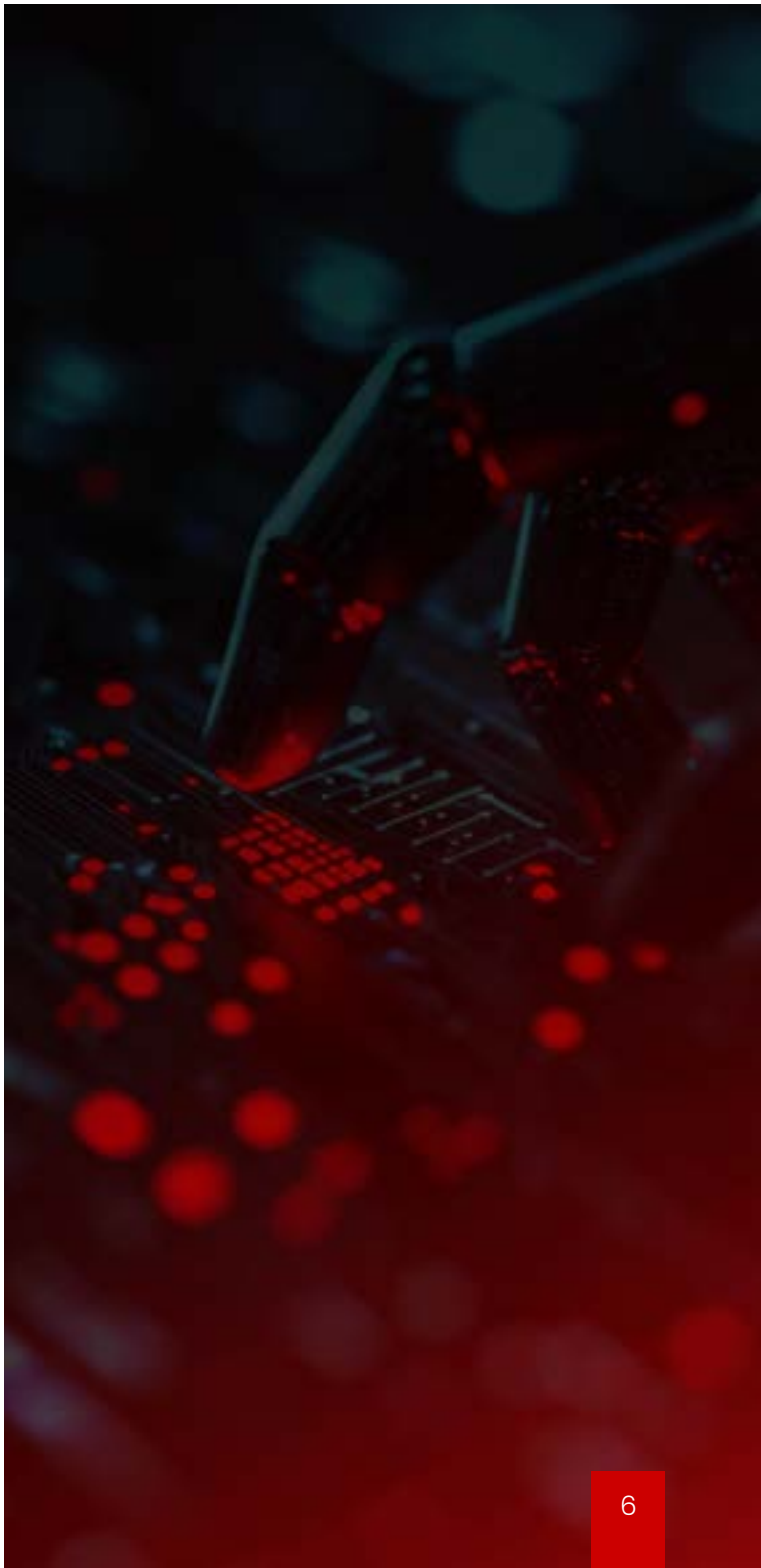
Prediction 4: Exploitation of Legacy Vulnerabilities

TRUE

PROOF

Cyble's forecast of continued exploitation of historical vulnerabilities was validated by persistent attacks targeting unpatched systems. Key examples included:

- **ZeroLogon (CVE-2020-1472):** A critical vulnerability in Microsoft's Netlogon protocol that allows attackers to impersonate any computer, including the domain controller itself, and gain administrative access. Despite being disclosed in 2020, it remains a target for exploitation due to unpatched systems.
- **Log4Shell (CVE-2021-44228):** A severe vulnerability in the Apache Log4j 2 library, enabling attackers to execute arbitrary code on affected systems. Its widespread use in various applications has led to continued exploitation attempts.
- **F5 BIG-IP Vulnerability (CVE-2020-5902):** A critical remote code execution vulnerability in F5 Networks' BIG-IP Traffic Management User Interface (TMUI). Attackers have continued to exploit this flaw in unpatched systems.
- **Fortinet FortiOS and FortiProxy Vulnerability (CVE-2018-13379):** A path traversal vulnerability in Fortinet's FortiOS SSL VPN web portal, allowing unauthenticated attackers to download system files. Despite its age, it remains a common target for exploitation.
- **Microsoft Exchange Server Vulnerabilities (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065):** A series of vulnerabilities in Microsoft Exchange Server that allow attackers to access email accounts and install malware. These continue to be exploited in unpatched systems.
- **CISA's KEV Catalog:** CISA's Known Exploited Vulnerabilities Catalog highlights numerous instances where threat actors have exploited historical vulnerabilities, emphasizing the need for timely patching.



Prediction 5: Increase in Cyber Incidents in India and U.S.

TRUE

PROOF

Both India and the U.S. experienced a sharp rise in cyber incidents, as Cyble predicted. These attacks targeted critical sectors and infrastructure, causing widespread disruption:

U.S.:

- **Salt Typhoon Cyberattack:** Hackers linked to the Chinese government infiltrated major internet service providers, including AT&T and Verizon, compromising sensitive information and raising concerns about national security.

  Read: Chinese Hackers Exploit Telecom Networks to Spy on US

- **Krispy Kreme Breach:** A cyberattack in November disrupted online operations, significantly impacting the company's digital sales channels.

  Read: Krispy Kreme Cyberattack Disrupts Online Orders; Company Responds to Data Breach

- **Change Healthcare Ransomware Attack:** In February, a ransomware attack led to widespread operational challenges across the U.S. healthcare system.

  Read: Change Healthcare Data Breach: Over 110 Million Potentially Affected, Free Credit Monitoring Offered

India:

- **Ransomware on Cooperative Banks:** A ransomware attack on C-Edge Technologies disrupted payment systems for nearly 300 local banks, prompting intervention by the Reserve Bank of India.

  Read: Ransomware Attack Hits 300 Banks: All You Need to Know

- **Polycab India Limited Attack:** The wire and cable manufacturer's IT infrastructure was compromised, underscoring the vulnerabilities of industrial sectors.

  Read: Exploring the Indian Cyberthreat Landscape: Top 15 Cyberattacks that Rocked India

Prediction 6: Collaboration Among Threat Actors

TRUE

PROOF

- **Ransomware-as-a-Service (RaaS):** The proliferation of RaaS models has facilitated collaboration among cybercriminals, enabling less skilled actors to launch sophisticated attacks. But the most prominent and recent case study is that of Iranian state actors collaborating with ransomware attackers.

  Read: Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations

Prediction 7: Persistence of Cybercrime Forums

TRUE

PROOF

- **BreachForums Shutdown:** In May 2024, the FBI, in collaboration with international law enforcement, seized the notorious cybercrime forum BreachForums, disrupting a major platform for trading stolen data.

  Read: FBI Seized BreachForums' Web Domains and Telegram Accounts

- **Emergence of New Forums:** Following the takedown of BreachForums, new platforms quickly surfaced to fill the void, indicating the resilience and adaptability of cybercriminal communities.

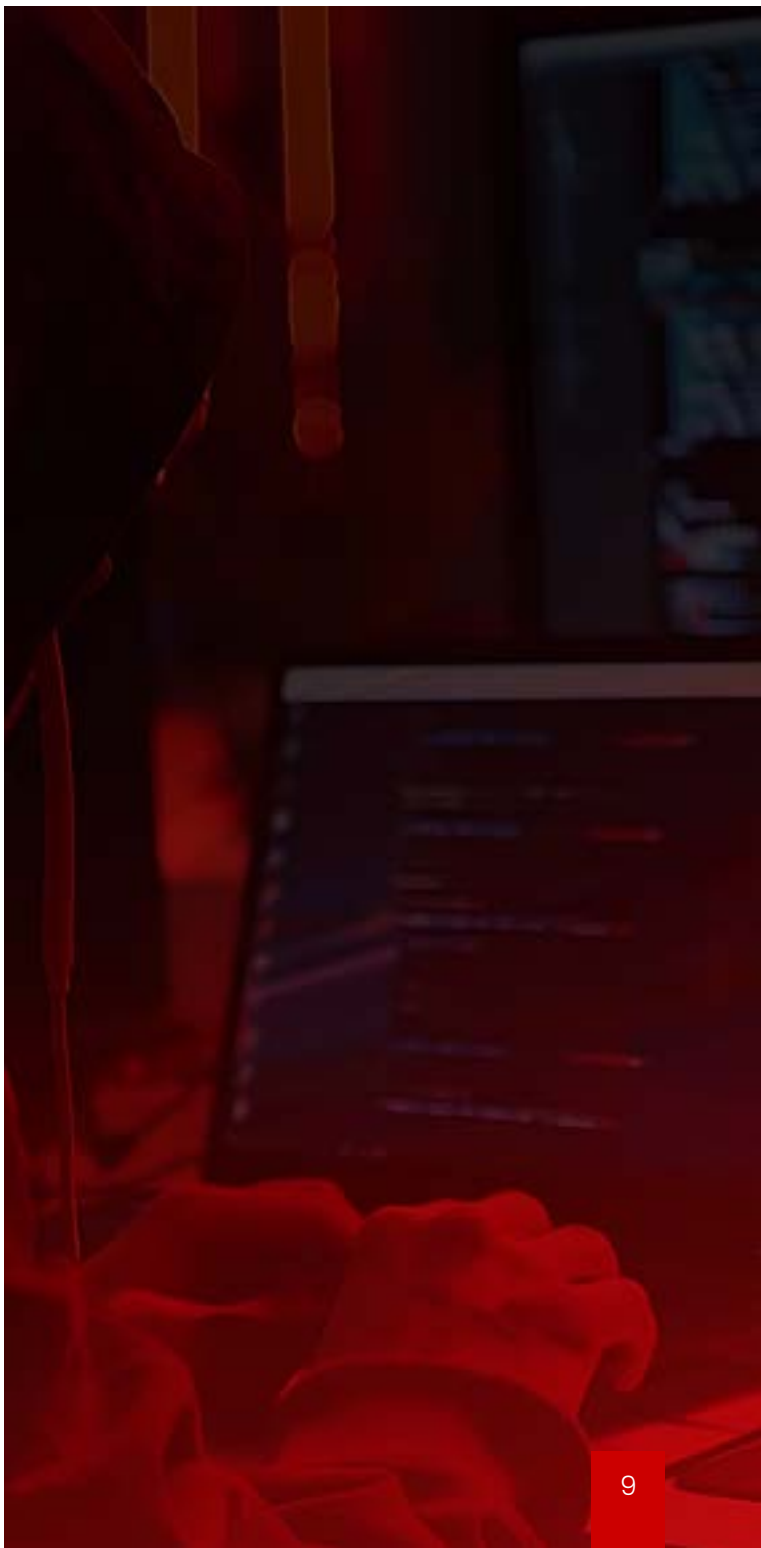
  Read: Threat Actor USDoD Announces Creation of 'Breach Nation', Following BreachForums Take Down

- **Nemesis Market Takedown:** German authorities have taken decisive action by shutting down Nemesis Market, a notorious dark web marketplace known for facilitating illegal activities such as drug trafficking, data theft, and cybercrime services.

  Read: Major Victory Against Cybercrime: Nemesis Market Shut Down by German Authorities

- **Operation Cronos:** An international task force disrupted the LockBit ransomware group, but successor groups and forums emerged, continuing illicit activities.

  Read: Operation Cronos: Law Enforcement Clamps Down on LockBit Network, Freezing $113M in Bitcoin



Prediction 8: Evolution of Ransomware Tactics

TRUE

PROOF

- **AI-Driven Phishing:** Ransomware groups employed AI to craft more convincing phishing emails and social media messages, increasing the success rate of their attacks.

  Read: Generative AI Application Scams Flourish on Facebook, Users Lured With Fake ChatGPT, Google Bard

- **SEC Breach Notifications:** Attackers exploited new SEC cybersecurity disclosure rules to pressure victims by threatening to report breaches, leveraging regulatory requirements as extortion tools.

  Read: Alphv/BlackCat SEC Complaint: A Desperate Move, Pressure Tactic, or Exploiting Regulations?

- **Targeting Critical Infrastructure:** Ransomware attacks increasingly focused on critical infrastructure sectors, aiming to cause maximum disruption and compel swift ransom payments.

  Read: Iranian State Hackers Act as Access Brokers for Ransomware Gangs, Target U.S. and Allies' Critical Infrastructure

Prediction 9: Ongoing Hacktivism Amid Global Conflicts

TRUE

PROOF

- **Pro-Palestinian Hacktivism:** Amid Middle Eastern tensions, hacktivist groups launched cyberattacks against organizations perceived as supporting opposing sides, disrupting services and defacing websites.

  Read: Cyber Warfare Surges as Over 35 Hacktivist Groups Join Israel-Palestine Conflict

- **Pro-Ukraine Cyber Operations:** In response to the conflict in Ukraine, hacktivist collectives targeted Russian government websites and state media, aiming to disrupt operations and spread pro-Ukraine messages.

  Read: Pro-Ukrainian Hackers Strike Russian State TV on Putin's Birthday

- **Environmental Hacktivism:** Hacktivists attacked corporations accused of environmental harm, leaking internal documents to raise awareness and pressure for change. Guacamaya is a hacktivist group acting in defense of the abuse performed on the territory and against the indigenous people of Central America. Their main goal is to exfiltrate compromised information from companies or organisms.

  Read: Hack-and-leak operations in Latin America: the case of Guacamaya

- **Anti-Government Protests:** In various countries, hacktivists targeted government websites to protest policies, using cyberattacks as a form of digital civil disobedience.

  Read: NATO Faces Escalating Cyberthreats: From Espionage to Disinformation

Prediction 10: Challenges in Cybersecurity Adaptation

TRUE

PROOF

- **AI-Enhanced Attacks:** The integration of AI into cyberattacks increased their sophistication, challenging traditional defense mechanisms.

  Read: KnowBe4 Uncovers Fake Employee: How a North Korean Hacker Was Hired into the Team

- **Supply Chain Vulnerabilities:** Attacks on software supply chains became more prevalent, compromising widely used applications to distribute malware.

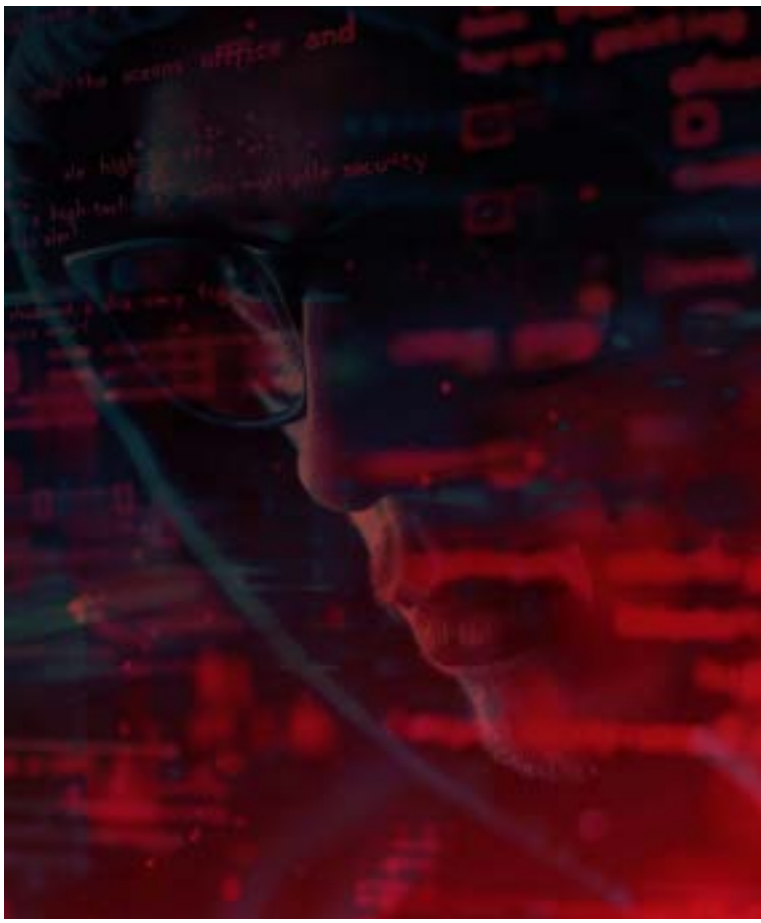
  Read: Polyfill Supply Chain Attack Could Affect 4% of the Web; Shutdowns, DDoS Attacks Among Spillover

- **Zero-Day Exploits:** The rise in zero-day vulnerabilities exploited by attackers outpaced the development of patches, leaving systems exposed.

  Read: MITRE Hit in Massive Supply Chain Attack: State-Backed Hackers Exploit Zero-Days

- **Talent Shortage:** The cybersecurity industry faced a significant talent gap, hindering efforts to keep up with evolving threats.

  Read: The Alarming Skill Shortage in India's Booming Cybersecurity Sector



Looking Ahead: Cyble's 2024 Annual Threat Landscape Report

As 2024 concludes, Cyble's accurate predictions underscore its role as a leading authority in cybersecurity intelligence. The **Annual Threat Landscape Report 2024**, slated for release in January 2025, promises to provide an in-depth analysis of emerging trends and actionable strategies to combat future threats.

Organizations worldwide are eagerly anticipating this report, which will undoubtedly serve as a critical resource for navigating the increasingly complex cybersecurity landscape. With a proven track record, Cyble is poised to continue shaping the future of cybersecurity, offering unparalleled insights to safeguard digital ecosystems.

Cyble Inc. is a cybersecurity company specializing in dark web monitoring and threat intelligence services. Cyble leverages proprietary AI-based technology to help enterprises, federal bodies, and individuals stay ahead of cybercriminals. The company is known for its expertise in tracking cyber threats, data breaches, and other malicious activities.

See Cyble in Action

10080 North Wolfe Road, Suite SW3-200, Cupertino, CA 95014 | contact@cyble.com | +1 888 673 2067