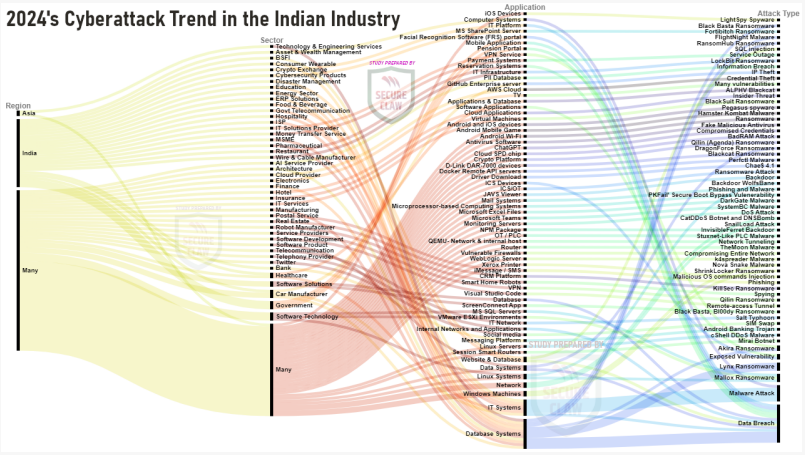
Indian Industry Cybersecurity Report 2024: Trends, Insights, and 2025 Recommendations by SecureClaw

In 2024, India made huge progress in cybersecurity through enhanced frameworks, AI-ML, and international cooperation, yet there are sophisticated cyber threats.



2024's Cyber Threats of India by SecureClaw

MUMBAI, MAHARASHTRA, INDIA, January 3, 2025 /EINPresswire.com/ -- SecureClaw's Cyber Threat Advisory team has studied more than 5000 cyber-attack news stories worldwide in the year 2024, and here is a snapshot of its annual report. These diagrams showing analysis of India's industry-targeted cyberattack trends were observed through various media sources and research articles. Few were directly from India, whereas few sources were generic about entire Asia, and many cyberattacks were happening in industries worldwide, not specific to a particular region. The Indian Computer Emergency Response Team (CERT-In) has issued new guidelines under section 70B of the Information Technology Act, 2000, requiring all cybersecurity incidents to be reported within six hours of noticing or being informed about them. These guidelines are part of an effort to enhance the country's cybersecurity posture and ensure timely responses to potential threats. In reality, many organizations never report the cyber incident because of concerns like fear of damage to their reputation. Hence, no one is able to identify exact statistics of the cyber-attack trends.

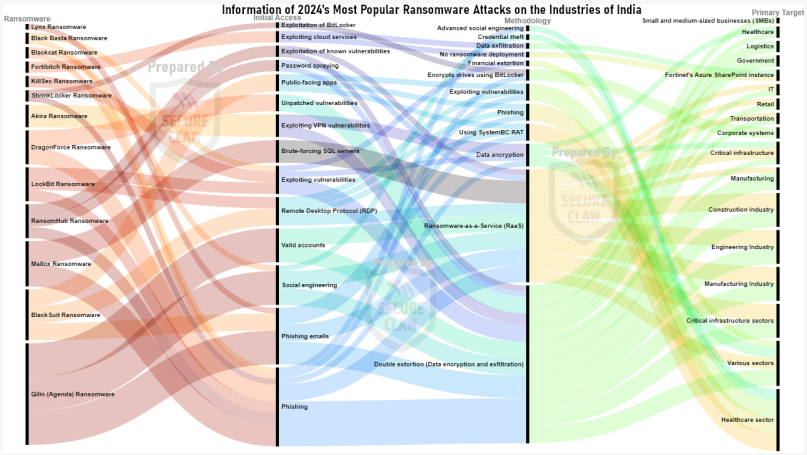
> Cybersecurity is a right of every business, regardless of its size, location or revenue. SecureClaw is providing a cost-effective, easy-to-adopt, and tailored BDSLCCI framework 3.0 for SMEs worldwide!"
>
> *Dr. Shekhar Pawar, Founder & CEO, SecureClaw*

There are two cyber threat terms mostly visible in many cyber-attack news, one is "Malware" and another one is "Ransomware".

Malware is malicious software designed to harm computer, server, client, OT, IoT, or network confidentiality. Common types include viruses, worms, trojans, ransomware, spyware, adware, and rootkits. Malware can infiltrate systems through phishing emails, infected files, malicious websites, or exploiting software vulnerabilities. Once installed, it can steal, encrypt, or delete data, hijack core functions, spy on user activity, and lock users out until a ransom is paid.

2024's Malware Threats of India by SecureClaw

Ransomware attacks initially focused on encrypting victim systems or data and demanding ransom for the decryption key. However, gangs have since evolved to include double and triple extortion techniques. Double extortion involves encrypting data and taking a backup before encryption, threatening to leak it online. Hence, only having a backup ready to restore doesn't help the victim. In triple extortion, attackers use stolen data to target customers or business partners through DDoS attacks. Ransomware attacks can be costly, with average costs reaching millions of dollars, and pose a significant threat due to their speed and difficulty in tracing attackers.



2024's Ransomware Threats of India by SecureClaw

FlightNight is a cyber espionage campaign targeting Indian government and the energy sector, using modified HackBrowserData tool to exfiltrate sensitive information via Slack channels and phishing emails disguised as official invitations.

LightSpy, a sophisticated spyware targeting iOS devices, has evolved to steal sensitive data from apps like Telegram and WeChat. It is distributed through compromised websites and uses a loader to download plugins.

Black Basta, a ransomware-as-a-service (RaaS) variant, uses a double-extortion model to encrypt data and threatens to publish it unless a ransom is paid. It has targeted over 500 organizations across sectors like healthcare and critical infrastructure.

RansomHub, also known as Cyclops and Knight, uses a double-extortion model and has

impacted over hundreds of victims across critical infrastructure sectors.

Akira, a double-extortion ransomware targeting Windows and Linux systems, has impacted over 250 organizations.

LockBit, a prolific RaaS group, has been responsible for numerous ransomware attacks since 2019, using advanced techniques to gain initial access, steal, and encrypt data.

Fortibitch is a new cybercriminal gang using new methodology for getting ransom from its victims. It was observed that instead of installing ransomware-related malware, this gang was using unauthorized access for database breaches.

According to Dr. Shekhar Ashok Pawar, who has a doctorate in cybersecurity from SSBM Geneva, Switzerland, and is the founder of SecureClaw, only antivirus or firewall technical controls are not enough in today's sophisticated cyberattacks. SecureClaw has observed that despite having such technical controls, organizations are undergoing ransomware. Organizations must adopt defence in depth methodologies to build better cybersecurity posture. It should have strategic alignment of the technical, administrative, and physical security areas. It should consider at least few control areas such as Preventive, Detective, Deterrent, Recovery and Corrective. Preventive controls help to avoid any incident from occurring. Detective controls find information and specifics related to the actions of an occurrence. Deterrent controls act as a strategy or measure to deter a possible miscreant. Recovery controls put in place to rapidly return the environment to normal functioning. Corrective controls fix systems or components following an incident.

There are below key areas which needs attention towards cybersecurity adoption.

(1) Cyber-attacks can cause significant damage to an organization's reputation, trust, and share market price.
(2) Organizations can lose their productive time while undergoing cyber-attacks.
(3) Cybercriminals may sell an organization’s intellectual property (IP), such as source code, or technical designs on the dark web.
(4) The Digital Personal Data Protection (DPDP) Act in India aims to protect personal data and ensure privacy. Non-compliance can result in fines up to □250 crore (approximately $30 million). Cybersecurity controls implementation can help protect sensitive data.
(5) Adoption of a cybersecurity framework or standard is recommended for cyber insurance, reducing premium costs.
(6) Cyber-attacks on service providers can impact the entire ecosystem or allow cybercriminals to hack big organizations. Generally, big organizations outsource their operations or a few areas to other small and medium enterprises, but it is important to check they are cyber-secured.

Generally, micro, small, and medium enterprises (MSMEs), or small organizations like institutes or hospitals, are facing several challenges while adopting existing cybersecurity standards or frameworks. It includes less funding, a lack of cybersecurity knowledge, and available

cybersecurity standards that are not specific to their business's domain requirements, making it less attractive for return on investment. In that case, SecureClaw is providing the Business Domain Specific Least Cybersecurity Controls Implementation (BDSLCCI) cybersecurity framework, providing tailored cybersecurity controls depending on the organization's domain's specific needs. BDSLCCI is very helpful for MSMEs, startups, or any such kind of organizations, as it is very cost-effective, less time consuming while implementation, and provides cybersecurity for your business’s mission critical assets. It provides good return on investment justifying cybersecurity for sustaining and growing business success.

Apart from BDSLCCI Cybersecurity Framework for MSME kind of organizations, SecureClaw provides various services, including Vulnerability Assessment and Penetration Testing (VAPT), Virtual Chief Information Security Officer (Virtual-CISO), and Source Code Security Review (SAST) services.

Dr. Shekhar Ashok Pawar
SecureClaw Inc.
+1 218-718-2121
email us here
Visit us on social media:
Facebook
X
LinkedIn
Instagram
YouTube
Other
