CLOUDFLARE

Navigating the New Security Landscape: India Cybersecurity Readiness Survey

Over the last 12 months, the threat landscape in India has remained volatile with 55% of respondents indicating they had experienced data breaches[1].

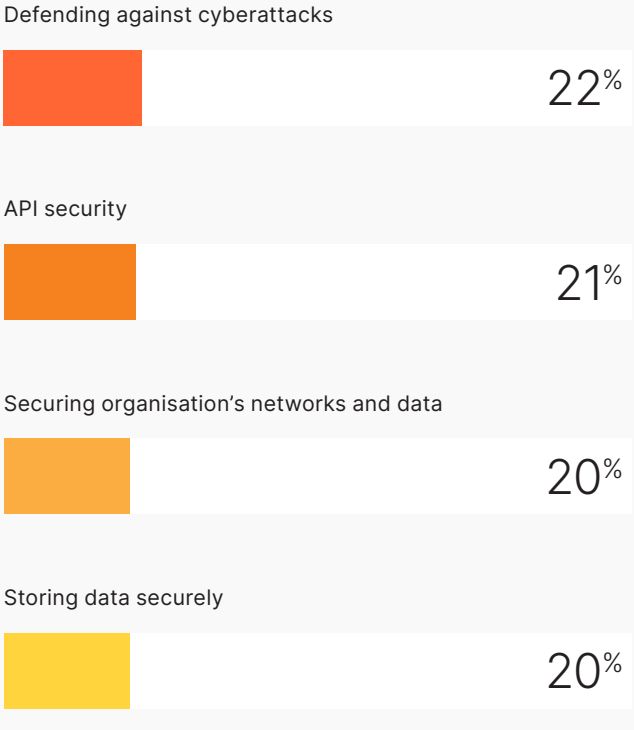
Among those that experienced data breaches, 82% indicated that the frequency had increased, with 52% of respondents claiming to have experienced 11 or more data breaches. Medium-sized organisations experienced the most data breaches (57%), while Healthcare (69%), Transportation (67%), and Business and Professional Services (62%) were the most commonly targeted industries.

Cybersecurity continues to be a critical area for IT spending, with 89% of respondents reporting that more than 10% of their organisation's IT budget was spent on cybersecurity, with the top cybersecurity priorities cited as defending against cyberattacks (22%), API security (21%), securing organisation's networks and data (20%), and storing data securely, while allowing appropriate use by the business (20%).

Where India stands out compared to peers in the region

	India	APJC
More likely to have experienced data breaches in the past 12 months	55%	41%
More prepared to prevent data breaches	95%	86%
More likely to be concerned about AI increasing the sophistication and severity of data breaches	93%	87%

Top cybersecurity priorities



Consolidation appears to be a commonly employed tactic, driven by challenges arising from the multitude of vendors; including pressure on human resources (61%), excessive time spent on repetitive tasks/non-critical cybersecurity functions (56%), and integration with other solutions and services (52%).

Web attacks (68%), malware (53%), and supply chain attacks (38%) were the top three attack vectors that resulted in data breaches, and customer data (37%), user access credentials (15%), and financial data (14%) were the most frequently targeted assets. Findings also show 93% of respondents are concerned about AI increasing the sophistication and severity of data breaches.

Despite the challenging threat landscape, there are signs that point to growing resilience. 95% of respondents feel they are prepared to prevent data breaches and 91% believe their organisation's cybersecurity posture was at least "somewhat mature". Organisations in Healthcare, Financial Services, and Transportation were most likely to be "highly prepared" when it came to preventing data breaches.

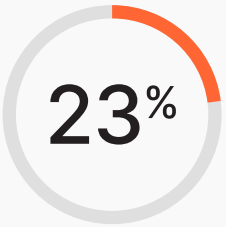
1. A data breach is an incident in which attackers gain unauthorised access to an organisation's applications, data and networks, whereas incidents are actions that can potentially compromise system integrity.

Zero Trust adoption is well underway, with 55% of respondents indicating their organisations are currently investing in Zero Trust solutions. Another 41% of respondents are planning to invest in Zero Trust over the next 12 months. Key investment drivers were mitigating user credential theft and phishing with multi-factor authentication (23%), securing vulnerable IoT devices (20%), and enhancing network performance by replacing VPNs (17%).

Other challenges faced by respondents included a lack of cybersecurity talent (49%) and the emerging threat posed by AI (46%). Respondents mainly evaluated their cybersecurity solutions based on the time taken to detect cyberattacks (64%) and respond to them (62%).

Ransomware remains a growing concern. 33% of respondents were concerned about ransomware, with compromising Remote Desktop Protocol (RDP) or Virtual Private Network (VPN) servers (55%) the most common means of entry.

Key investment drivers for Zero Trust



user credential theft and phishing with multi-factor authentication

securing vulnerable IoT devices

enhancing network performance by replacing VPNs

Resources devoted to regulation and compliance

52% of respondents' organisations are spending more than 5% of their IT budget to address regulatory and compliance requirements

59% of respondents in India reported spending more than 10% of their work week keeping pace with industry regulatory requirements and certifications

82% of respondents whose organisations experienced ransomware attacks within the past two years said their organisations paid ransoms, despite 89% of them having issued public pledges not to. Customer pressure (43%) was a major factor behind paying ransoms. However, respondents believed their organisations were at least "somewhat mature" in relation to mitigating ransomware threats via the deployment of employee training (96%), two-factor authentication (93%), and anti-malware software (93%).

Regulation and compliance also emerged as important themes in this year's study. 52% of respondents' organisations are spending more than 5% of their IT budget to address regulatory and compliance requirements. 59% of respondents reported spending more than 10% of their work week keeping pace with industry regulatory requirements and certifications. However, this investment in regulation and compliance has had a positive impact on organisations, such as improving the integrity of the organisation's technology and data (63%), improving the organisation's baseline privacy and/or security levels (61%) and improving the organisation's reputation and brand (59%).

Recommendations

With these study findings in mind, here are six recommendations for CISOs for the year ahead:

Streamlining solutions to reduce complexity

In last year's report, we suggested streamlining security architecture through SASE. This year, not only does that suggestion remain, but the evidence is clear: more solutions and IT vendors does not correlate with risk reduction. Organizations should be considering a more measured approach to minimize the number of solutions deployed and consolidate the number of IT vendors they obtain their solutions from.

Strengthen the weakest link in the chain

In today's global and interconnected environment, every organisation relies on the software supply chain. Applications are built on open-source code, APIs, and third-party integrations are all part of the increasing attack surface. This expansion of our attack surface is why onboarding a new partner means choosing to trust its entire development ecosystem, rather than just the tool itself. Moving from a perimeter-based security model to a Zero Trust model that trusts no one, assumes that attackers are within the network already, assesses users, devices and workloads based on identity and context can reduce risk associated with a breach in your supply chain. Look for partners who are committed to secure by design principles.

Limit the leverage for ransomware attackers and make plans for demands

Ransomware attacks are on the increase and CISOs and their Boards need to have a plan in place. Looking at the evidence of this study, that plan should not include paying the ransom because in almost every case, organizations that have done so have regretted their course of action. We recommend a strategy of minimizing lateral movement should a breach occur, leveraging Zero Trust capabilities. In addition, a robust resiliency program will reduce the leverage of an attacker's demands. Assurance begins with regular data backups, tested to ensure efficacy and completeness, of your most critical systems and data. Regular disaster recovery testing is critical to identify gaps and build the muscle to restore operations and reduce impact.

Prepare for AI fuelling a multiplication and intensification of attacks

AI will be used by attackers and CISOs need to have AI defensive strategies in place. Cybersecurity leaders should be wary of simply outsourcing the problem but there is definitely a case for examining talent models, governance frameworks, compliance requirements and monitoring usage. A key action all can take now is to review the terms of engagement with third party vendors to ensure their use of your data, in their AI models, is understood and aligns with your requirements. How do your current security tools combat an increase in AI attacks? Many Cloudflare products leverage our massive global network of threat intel to combat new threats proactively.

Shift investment from capital to operating expenditure

Budgets for most are under pressure and cybersecurity leaders need to be good fiscal stewards. Look at upskilling existing team members to align with your future state, reduce complexity and streamline processes. Explore opportunities to reorganize roles to maximize effectiveness while also reducing lag time. It is worth looking at outsourcing some of the functions to MSPs, shifting investment from a capital expense to an operating expense.

Get used to more scrutiny

Cybersecurity leaders are facing increasing scrutiny internally and externally, adding to their already-significant pressures. This scrutiny will continue and CISOs need to be diligent in seeking opportunities to comply with changing regulations (local or international) as well as being able to meet the needs of board members. Ensure your audit commitments are negotiated to clear scope and timelines to reduce tasks that don't add value to your customers nor reduce risk.

Move to a connectivity cloud

Cloudflare plays a crucial role in providing security everywhere by offering a new category of service, called the connectivity cloud, that connects and protects a company's people, apps, and networks. Through Cloudflare's broad portfolio of security offerings, such as application, API and network security, Zero Trust, and global threat intelligence, organisations can fortify their digital infrastructure against cyberattacks. An organisation can ensure the security of their online data and intellectual property, and protect the integrity of their brand.

These security services are built on Cloudflare's unified platform of programmable global cloud network services, which connects and protects a massive percentage of the world's Internet traffic and stops an average of 182 billion threats per day. This global cloud network minimises the risk of downtime and ensures high availability by providing redundancy and resilience against network outages and infrastructure failures.

To learn more about Cloudflare's suite of solutions and request a demo or POC from a sales representative, please visit: **cloudflare.com**. We will help evaluate your existing security posture and collaborate towards an action plan for strengthening your cybersecurity for your people, applications, devices, networks, and data.

Scan here to read the full report

* **Navigating the New Security Landscape: Asia Pacific Cybersecurity Readiness Survey** features findings from the security market across Asia Pacific, Japan and China. The study was conducted across 3,844 cybersecurity decision makers and leaders across 14 markets.