CLOUDFLARE

Spotlight: India

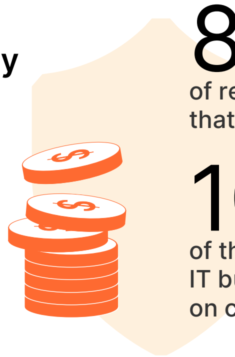
Navigating the New Security Landscape:
Asia Pacific Cybersecurity Readiness Survey

Complex and evolving security threats

55% experienced data breaches, of which

82% indicated that the frequency increased over the last 12 months

Cybersecurity continues to be a top priority



80% of respondents reported that more than

10% of their organisation's IT budget was spent on cybersecurity

Top three attack vectors that resulted in breaches:

68% Web attacks

53% Malware

38% Supply chain attacks

Top cybersecurity priorities:

22% Defending against cyberattacks

21% API Security

20% Securing organisation's networks and data / Storing data securely

Top issues with current cybersecurity architecture:

Lack of visibility into the attack surface

50%

Inconsistent WAF & WAN security policies

42%

Poor end user experience/ latency challenges

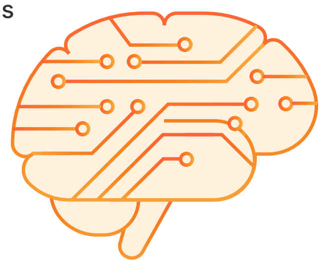
40%

AI has altered the cybersecurity landscape

93% are concerned about AI increasing the sophistication and severity of data breaches

91% believe they can stay ahead of threat actors leveraging AI

96% believe their organisations are at least somewhat prepared to prevent data breaches powered by AI



Ransomware a clear and present danger

65% have paid ransoms in the last 24 months

55% say an attacker compromising Remote Desktop Protocol or Virtual Private Network servers is the most common means of entry for ransomware

43% cite pressure from customers to restore systems as the top reason why they ended up paying ransom

Data breaches are breaking the bank

51% report combined losses of more than USD 1 million due to data breaches over the past 12 months

Zero Trust is firmly on the agenda

55% indicate their organisations are currently investing in Zero Trust solutions

41% are planning to invest in Zero Trust over the next 12 months

Maintaining regulatory compliance has benefits

52% spending more than

5% of IT budget to address regulatory/ compliance requirements

Most deployed Zero Trust solutions:

90% Multi-factor authentication

90% Data encryption

88% Secure web gateway

Key positive impact of investment in compliance:

Improving integrity of organisation’s technology and data 63%

Improving organisation’s privacy/security 61%

Improving organisation’s reputation and brand 59%

Study Methodology: The findings of this study are drawn from a double-blind survey conducted in June 2024 of 3,844 leaders responsible for cybersecurity in their organisations across 14 markets, key industries and organisations ranging from 250 - 2500+ in terms of employee size.

Read the full report here:

| 1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com