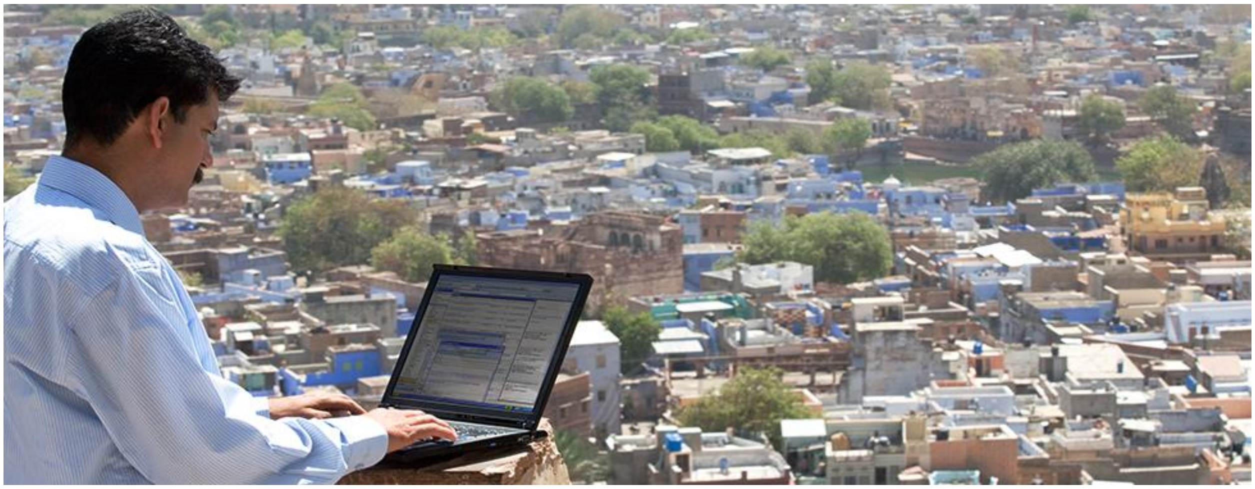
Security in India: Enabling a New Connected Era



India's economy is growing rapidly, and the country is expanding its network infrastructure to support digitization. India's "leapfrogging" mobile development is helping many unconnected areas adopt the Internet wirelessly. However, as the technology evolves, organizations must increase their focus on protecting themselves from cybercriminals. A shortage of IT talent, a predicted increase in cybercrime, and the lack of solid regulatory frameworks for cybersecurity add to the list of concerns.

- Security professionals appear confident that their threat defenses are solid. However, they may be underestimating the potential impact of cyber attacks.
- Indian organizations show a strong reliance on security tools and point systems but need to integrate them to gain better protection and more visibility into threats.
- Outsourcing and use of the cloud are popular, which may be a result of the tight market for IT labor.

Organizations in India have to keep building an internal awareness of security threats. They must also strengthen their defenses–before, during and after an attack.

Major Findings

In this paper, Cisco experts analyze the IT security capabilities in India, using data from the Cisco Security Capabilities Benchmark Study.[1] In our analysis, we found that:

- Indian organizations appear confident in their ability to protect their networks.
- Security professionals' confidence may be at odds with the reality of the security environment in the country. For example, cybercrime is predicted to double in 2015.
- Indian organizations are more likely to use cloud-based security tools than organizations in other countries. For example, 60 percent of Indian organizations use cloud-based web security. Only 34 percent of organizations outside India do.

[1] For more information on this study and the other white papers in this series, see the final sections of this document.

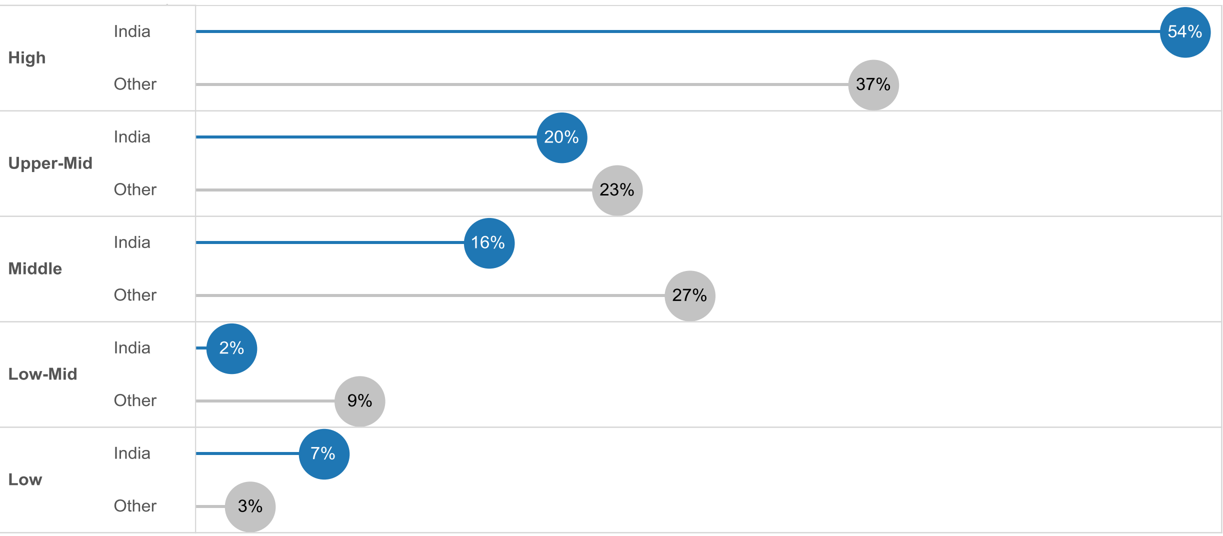
- Unlike chief information security officers (CISOs) and security operations (SecOps) managers in other countries, those in India work closely together. As a result, they tend to have similar views on their organization’s security sophistication.

Confidence in Tools to Prevent Breaches

Indian security professionals purchase a broader set of threat defense tools for their organizations than do their counterparts elsewhere in the world, according to our study. But organizations may be favoring point solutions over true holistic security architectures, which would create a better framework for secure network operations.

Because they adopt many security tools, Indian security professionals feel confident about their readiness to protect their networks against cyber attacks. Based on their responses to our study, we classified 74 percent of the organizations in India as either upper-middle or high in terms of security sophistication, compared with 60 percent outside India (Figure 1).

Figure 1. Perceived Level of Security Sophistication in Indian and Non-Indian Organizations (in Percentages of Respondents)



To Cisco’s local security experts, this level of confidence in their readiness is higher than expected, given these trends:

- India does not yet have comprehensive cybersecurity regulations. In addition, organizations in India are not required by law to report breaches. The country created a national cybersecurity policy in 2013, but it may require further work. Policy improvements are under discussion.
- There is a shortage of skilled IT talent. The most skilled security professionals may leave the country to seek higher salaries elsewhere, making it difficult for Indian organizations to properly staff their security operations. The gap between the available security talent and open positions may reach 1 million professionals by 2020.[2]

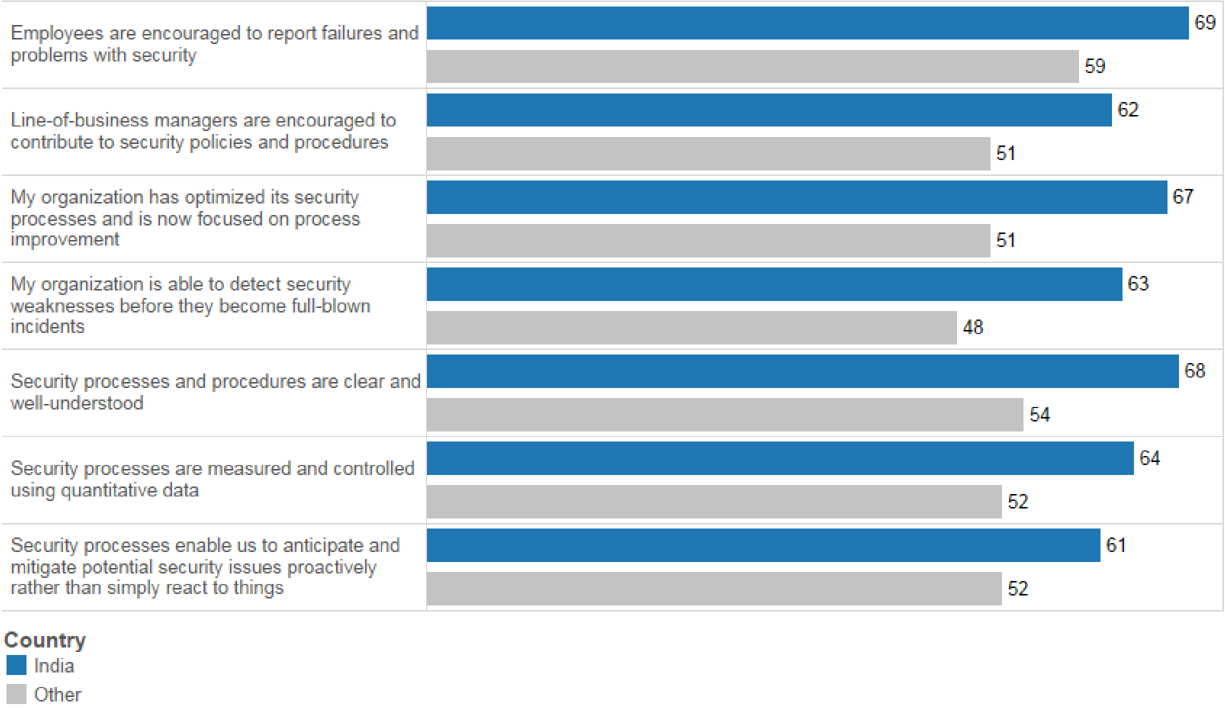
Given these shortcomings, the number of Indian organizations ranking high in terms of perceived security sophistication may indicate some overconfidence. For example, 67 percent of Indian organizations say that their security processes are optimized, compared with 51 percent of organizations elsewhere. And 68 percent of Indian

[2] “Cyber security: 1 million cyber security professionals needed by 2020,” *The Economic Times*, August 25, 2015: http://articles.economictimes.indiatimes.com/2015-08-25/news/65847438_1_cyber-security-ethical-hacking-information-security.

organizations say that their security processes are clear and well understood, compared with 54 percent of organizations elsewhere in the world (Figure 2).

Cybercrime in India is expected to double in 2015.[3] Many organizations will face a reality check.

Figure 2. Confidence in the Security Culture of Organizations (in Percentages of Respondents)

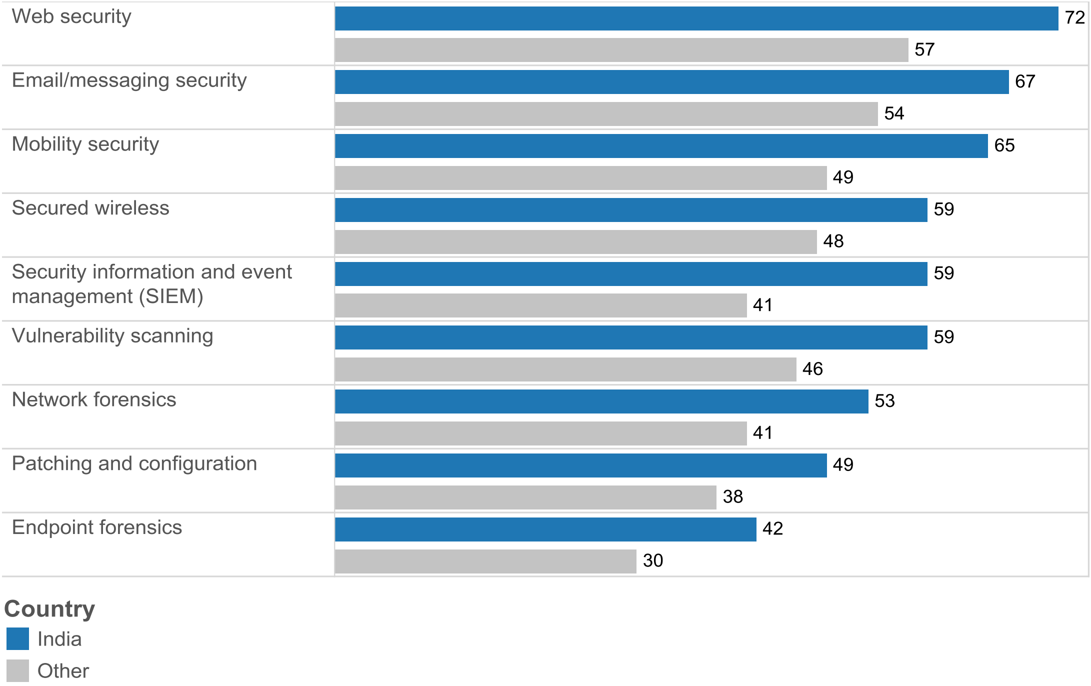


Stronger Threat Defenses in Use

Indian organizations use stronger threat defenses than do organizations in other countries. Seventy-two percent of Indian organizations use web security; only 57 percent of non-Indian organizations do. In addition, 65 percent of organizations in India use mobile security, compared with 49 percent of organizations outside India (Figure 3).

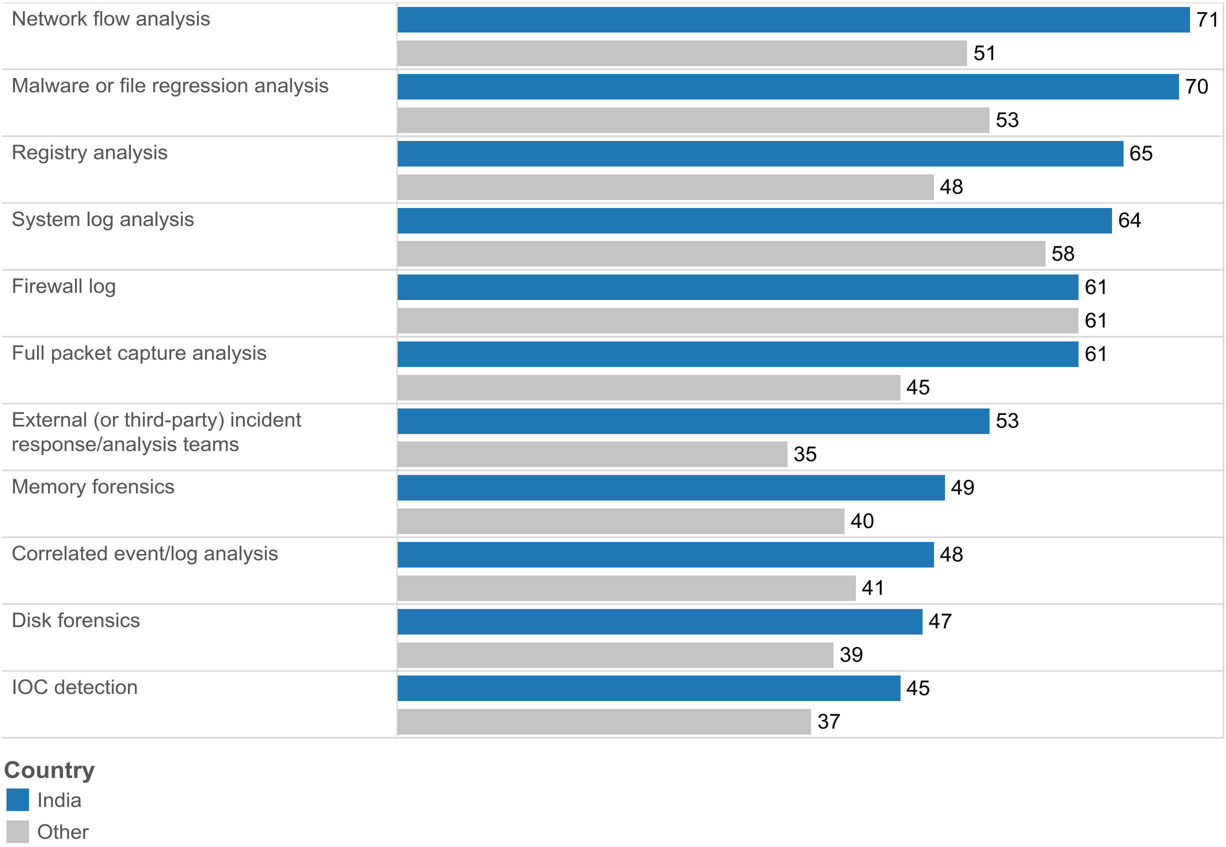
[3] "Cyber Crimes in India May Double in 2015: Study," IBN Live.com, January 4, 2015: http://www.ibnlive.com/news/india/cyber-crimes-in-india-may-double-in-2015-study-734197.html.

Figure 3. Use of Various Threat Defense Tools (in Percentages)



Indian organizations are more likely than those in other countries to adopt tools to analyze compromises and eliminate incident causes. For example, 71 percent of Indian security professionals say they use network flow analysis, compared with 51 percent of their counterparts (Figure 4).

Figure 4. Use of Various Processes to Analyze Compromises (in Percentages)

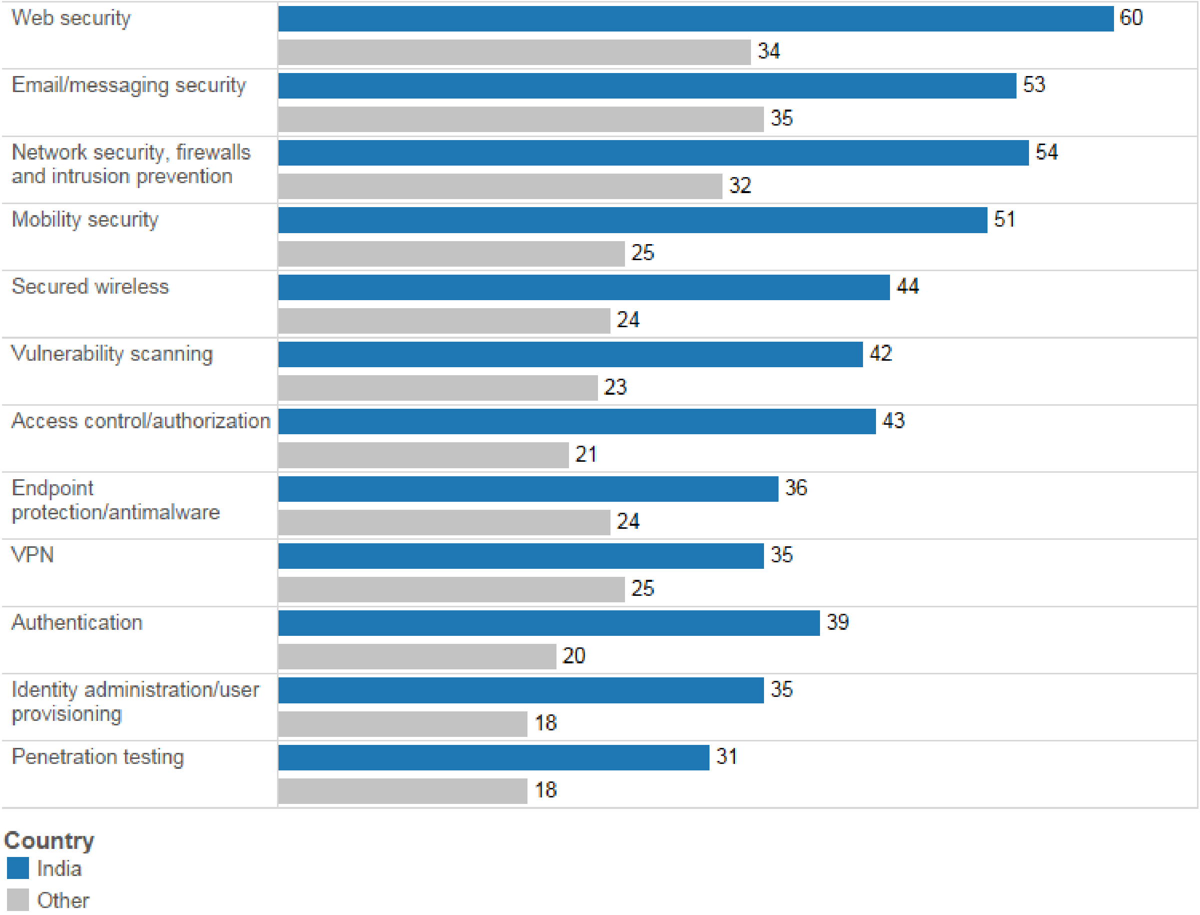


The greater use of broad threat defenses by Indian organizations may point to a reliance on tools instead of strategies to boost protection. In turn, the higher adoption of threat defenses likely plays a role in Indian security professionals' views of their organizations as highly sophisticated. However, our experts caution that tools alone cannot provide complete protection. Organizations require a strong security architecture and established processes to help improve the effectiveness of tools.

Greater Reliance on Cloud and Third-Party Services

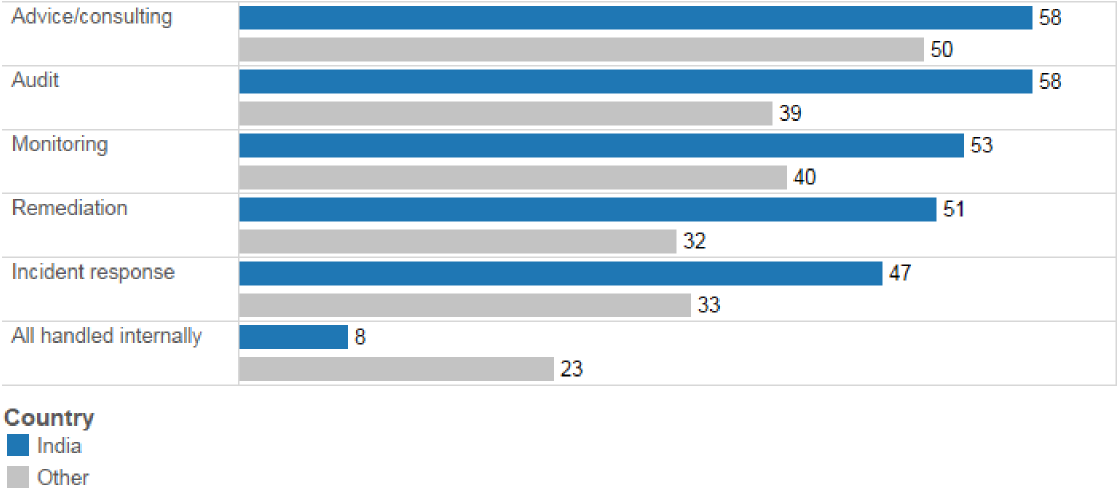
Indian organizations have adopted more cloud-based tools than organizations in other countries. For example, 60 percent of Indian organizations use cloud-based web security; just 34 percent of organizations outside India do. In addition, 51 percent of Indian organizations use web-based mobile security, double the percentage of non-Indian organizations (Figure 5).

Figure 5. Use of Various Cloud-Based Tools (in Percentages)



Indian organizations are also more likely to outsource some security services. Fifty-eight percent of Indian organizations say they outsource advice and consulting services, compared with 50 percent of organizations in other countries. In addition, 58 percent of Indian organizations outsource audit services, compared with 39 percent of non-Indian organizations (Figure 6).

Figure 6. Organizations Outsourcing Various Security Services (in Percentages)



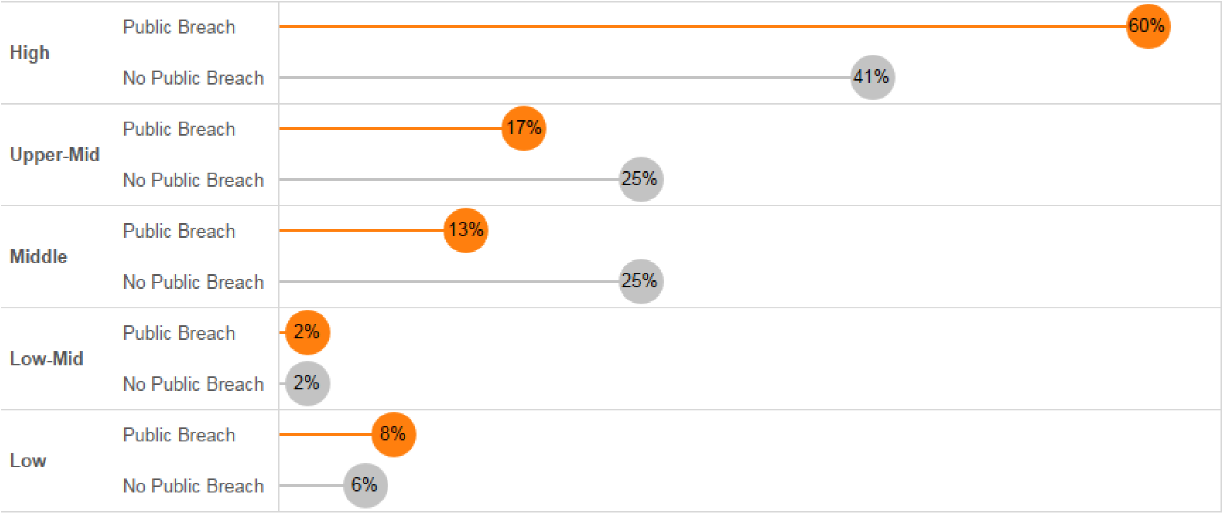
Their willingness to seek out cloud and outsourced solutions may be in response to the shortage of IT professionals in the country, and it may reduce the need for security personnel in-house.

Higher Sophistication for Publicly Breached Organizations

Seventy-four percent of Indian organizations say they have dealt with public scrutiny after a data breach. In other countries, 51 percent of organizations have dealt with such scrutiny. This finding is surprising considering that India does not require companies to report breaches. The surge in cybercrime in the past few years may be behind the increased exposure and scrutiny following a breach.

Indian organizations that have dealt with a public security breach rate themselves higher in sophistication than those that have not: 77 percent of organizations that have dealt with a breach are ranked upper-middle to high in terms of their security sophistication, and 66 percent of non-publicly-breached organizations are in this category (Figure 7). The higher ranking for publicly breached companies may be due to the increased security awareness that results from a public breach. The scrutiny of exposed vulnerabilities may motivate publicly breached companies to take action, while also giving them direction on which areas require improvement.

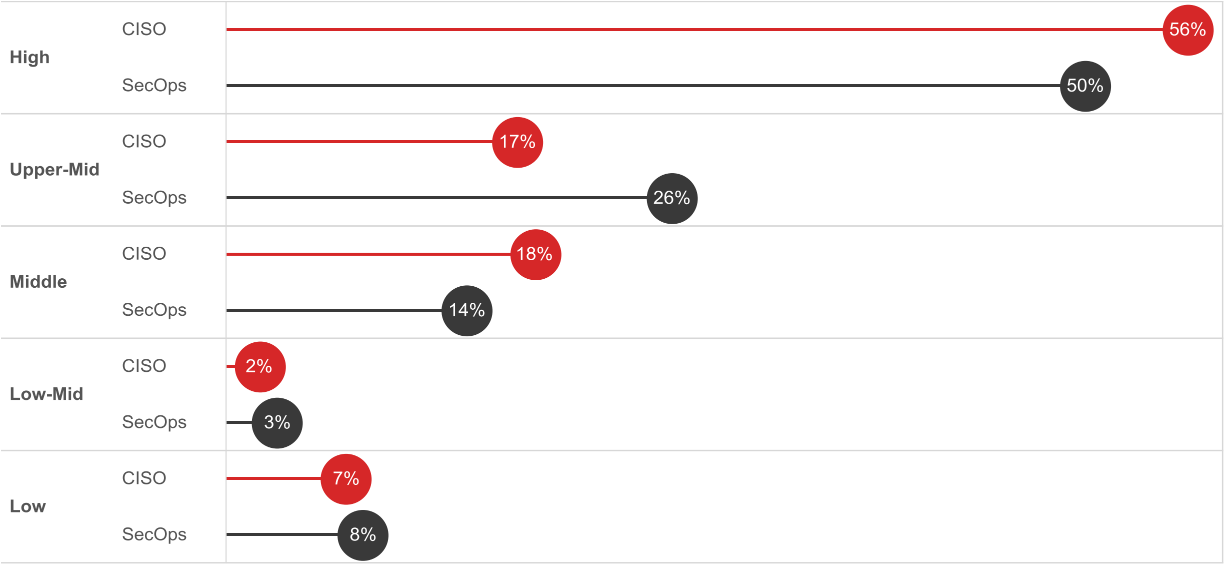
Figure 7. Level of Perceived Security Sophistication in Publicly Breached and Non-Publicly-Breached Indian Organizations



Close Alignment between CISOs and SecOps Managers

Unlike most countries we surveyed, India shows an alignment between CISOs and SecOps managers in terms of how they perceive their organization's security sophistication. Seventy-three percent of CISOs ranked their organizations as either upper-middle or high in sophistication, and 76 percent of SecOps managers did, too (Figure 8). These two groups of professionals are usually part of the same team in India, which could explain why they have similar views on the state of their operations.

Figure 8. Perception of Security Sophistication in Indian Organizations, by Role



Conclusion: Integrate Tools into Security Architecture

When it comes to protecting networks, adopting tools to fight threats is only half the battle. In India, organizations appear to be deploying many common threat defense tools. The next step is to integrate these tools into a more sophisticated security infrastructure. Point solutions can accomplish only so much. A comprehensive security architecture helps manage the full attack continuum.

Indian organizations are fortunate that CISOs and SecOps managers appear to be closely aligned in their understanding of their security readiness. They should build on this alignment to help raise the visibility of security needs at the executive level.

Security professionals should help build awareness across the business of the expected growth in cybercrime. They should also lead the implementation of countermeasures to protect their businesses against threats.

To prepare for this probable wave of attacks, Indian security professionals should:

- Assume that a breach will happen. Companies should have processes in place to detect and mitigate attacks and should gather intelligence to continuously strengthen their security strategy.
- Make sure that their defenses interoperate to increase their effectiveness and provide greater visibility into threats.
- Continue to explore ways to outsource security services or rely on third-party service providers. These measures may help make up for the lack of highly trained IT professionals.

Learn More

To learn how to become more resilient to new attacks and compete more safely in the digital age, get the Cisco 2016 Annual Security Report at www.cisco.com/go/asr2016.

To learn about Cisco's comprehensive advanced threat protection portfolio of products and solutions, visit www.cisco.com/go/security.

About the Cisco 2014 Security Capabilities Benchmark Study

The Cisco 2014 Security Capabilities Benchmark Study examines defenders across three dimensions: resources, capabilities, and sophistication. The study includes organizations across several industries, in nine countries.

In total, we surveyed more than 1700 security professionals, including chief information security officers (CISOs) and security operations (SecOps) managers. We surveyed professionals in the following countries: Australia, Brazil, China, Germany, India, Italy, Japan, the United Kingdom, and the United States. The countries were selected for their economic significance and geographic diversity.

To read findings from the broader Cisco Security Capabilities Benchmark Study referenced in this paper, get the Cisco 2015 Annual Security Report at www.cisco.com/go/asr2015.

The latest version of the study is now available in the Cisco 2016 Annual Security Report: www.cisco.com/go/asr2016.

About This White Paper Series

A team of industry and country experts at Cisco analyzed the Cisco 2014 Security Capabilities Benchmark Study. They offer insight on the security landscape in nine countries and six industries (financial services, government, healthcare, telecommunications, transportation, and utilities). The white papers in this series look at the level of maturity and sophistication of the survey respondents and identify the common elements that indicate higher levels of security sophistication. This process helped contextualize the findings of the study and brought focus to the relevant topics for each industry and market.

About Cisco

Cisco delivers intelligent cybersecurity for the real world, providing one of the industry's most comprehensive advanced threat protection portfolios of solutions across the broadest set of attack vectors. Cisco's threat-centric and operationalized approach to security reduces complexity and fragmentation while providing superior visibility, consistent control, and advanced threat protection before, during, and after an attack.

Threat researchers from the Collective Security Intelligence (CSI) ecosystem bring together, under a single umbrella, the industry's leading threat intelligence, using telemetry obtained from the vast footprint of devices and sensors, public and private feeds, and the open source community at Cisco.

This intelligence amounts to a daily ingestion of billions of web requests and millions of emails, malware samples, and network intrusions. Our sophisticated infrastructure and systems consume this telemetry, enabling machine-learning systems and researchers to track threats across networks, data centers, endpoints, mobile devices, virtual systems, web, email, and from the cloud to identify root causes and scope outbreaks. The resulting intelligence is translated into real-time protections for global customers.

The CSI ecosystem is composed of multiple groups with distinct charters: Talos, Security and Trust Organization, Active Threat Analytics, and Security Research and Operations.

To learn more about Cisco's threat-centric approach to security, visit www.cisco.com/go/security.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA 11/15