Cisco 2017 Security Capabilities Benchmark Study

India Findings for the Government Sector

India Findings for the Government Sector

To gauge the perceptions of security professionals on the state of security in their organizations, Cisco asked chief security officers (CSOs) and security operations (SecOps) managers in several countries and at organizations of various sizes about their perceptions of their own security resources and procedures. The Cisco 2017 Security Capabilities Benchmark Study offers insights on the maturity level of security operations and security practices currently in use, and also compares these results with those of the 2016 and 2015 reports. The study involved more than 2,900 respondents across 13 countries, including India.

In September 2017, the findings pertaining to 202 Indian respondents in the Cisco 2017 Security Capabilities Benchmark Study were published in a separate report. This report drills down further to present the findings and analysis for 22 respondents from the Indian Government Sector.

Around the world, governments are taking strong policy and practical measures to lead their respective countries into the Digital Age. As government establishments also turn digital, they are becoming prime targets of cyber attack.

Hence cyber security is now a key priority of governments everywhere. As one of the IT superpowers, India is very serious about defending its government and private organizations as well as its citizens from cyber threats. The National Cyber Safety and Security Standards is responsible for spreading awareness and education about safe online practices among the public, while the National Cyber Defence Research Centre is setting up research facilities and laboratories for the early identification and prevention of cyber attack.

When it comes to protecting its own organizations, the Indian government sector resorts to a plethora of solutions and vendors, using significantly larger numbers of both compared to the average Indian enterprise. There is a strong likelihood of these products not communicating well with each other and therefore compromising the organization's overall defenses.

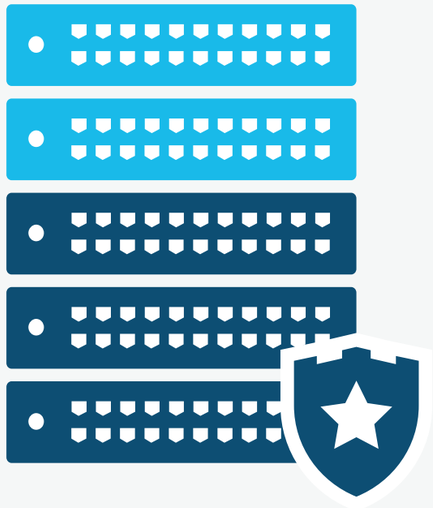
The presence of multiple solutions and vendors is also a drain on organizational resources. Worst of all, even after spending so much time and effort on managing the snarl, the organization is not assured of a fully effective security environment. The government sector needs to trim its list of point solution vendors and products and move towards an integrated security solution that is open, automated and simple.

Perceptions: Security Professionals are Confident about Technology, but cannot Leverage it Fully because of Constraints

In the Cisco 2017 Security Capabilities Benchmark Study, representatives of Indian organizations appeared very confident about their security technology, even though threat levels were rising. 69 percent of CISOs and security operations professionals said that their security infrastructure was very up to date and was constantly being upgraded with the best technologies available.

73 percent of Indian government organizations felt the same while the remaining 27 percent said that they replaced or upgraded their security technologies regularly despite not having the latest tools.

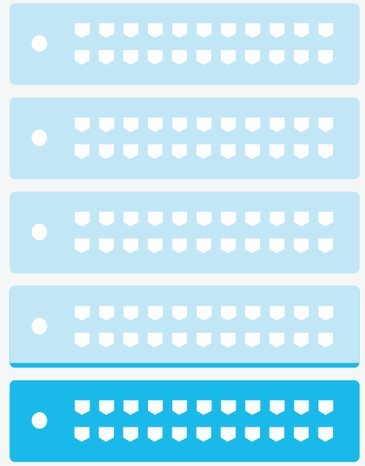
Figure 1. Percentages of Security Professionals in Government Sector Who Feel Their Security Infrastructure is Up to Date



Described as Very Up to Date

Best Technologies Available

73%



Described as Replaced/Upgraded on Regular Cadence

Not Equipped with Latest and Greatest Tools

27%

2016 (n=22)

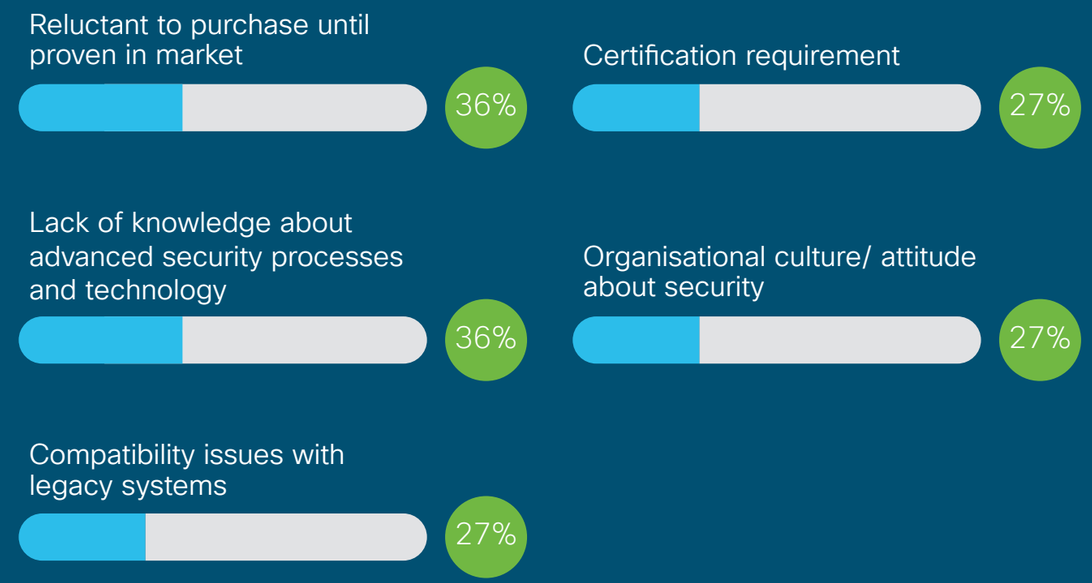
Source: Cisco 2017 Security Capabilities Benchmark Study

Constraints: Different Government Organizations are Prevented from Adopting Security Measures by Different Constraints, Including Reluctance to Purchase Unproven Solutions, Lack of Knowledge, Certification Requirements and Incompatible Legacy Technology

Being equipped with the latest tools and technologies does not mean that Indian organizations have an easy time implementing their security agenda. Security professionals face several obstacles, ranging from legacy system issues to lack of knowledge about advanced security processes and technology. In the survey, Indian organizations overall said that the biggest barrier to security was organizational culture and attitude, closely followed by compatibility issues with legacy systems.

Indian government organizations, however, were quite fragmented in their response. 36 percent of respondents said they were reluctant to invest in a solution that was not yet proven, and an identical number cited lack of knowledge about advanced security processes and technology as a major barrier to adoption. Compatibility problems with legacy systems, certification requirements and organizational culture and attitude were each named as a challenge by 27 percent of respondents. A matter of some concern was the fact that nearly 20 percent of respondents thought that their organizations were not a major target of attack, and also that 14 percent said security was not an executive level priority.

Figure 2. Biggest Obstacles to Security in Government Sector



2016 (n=22)

SHARE

Source: Cisco 2017 Security Capabilities Benchmark Study

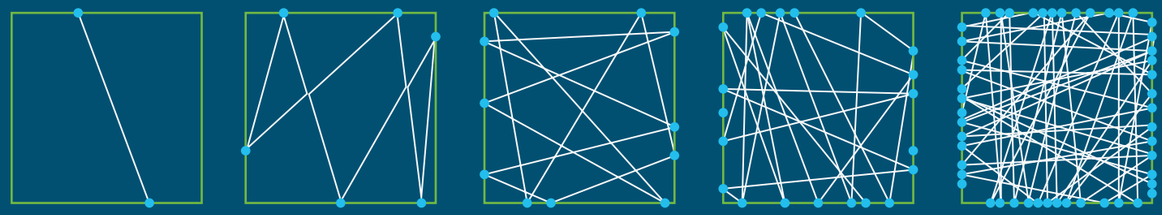
When it comes to the number of security products, more does not always mean better security. In fact, an abundance of point solutions can make an organization more vulnerable to attack, especially when those solutions don't communicate or integrate seamlessly with each other. Unfortunately, Indian organizations – and for that matter, organizations around the world – have accumulated too many point products over the years, opening up gaps in time and space that hackers can exploit.

Government establishments fare even worse than the average Indian enterprise on this front. The study found that 56 percent of Indian organizations used 6 or more vendors and 69 percent of organizations used 6 or more security products. In comparison, 73 percent of respondents from the government sector said they used 6 or more vendors and a massive 82 percent said they used 6 or more products.

Figure 3. Number of Security Vendors and Products Used in Government Sector

Number of Security Vendors in Security Environment

2016 (n=22), Graphic Rounded to Nearest Whole Number

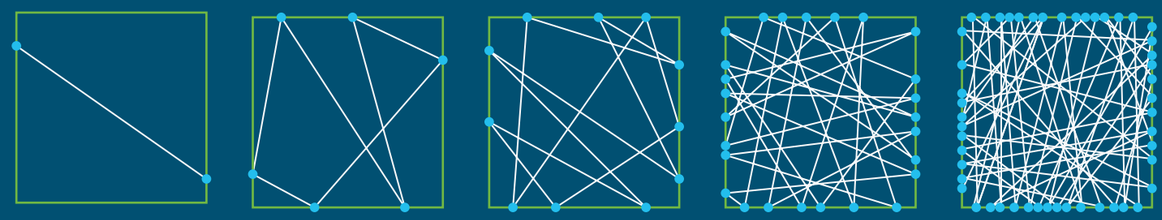


1–5 Vendors	6–10 Vendors	11–20 Vendors	21–50 Vendors	Over 50 Vendors
27%	18%	14%	18%	23%

73% Use More Than 5 Vendors

Number of Security Products in Security Environment

2016 (n=22), Graphic Rounded to Nearest Whole Number



1–5 Products	6–10 Products	11–25 Products	26–50 Products	Over 50 Products
18%	18%	9%	14%	41%

82% Use More Than 5 Products

Source: Cisco 2017 Security Capabilities Benchmark Study

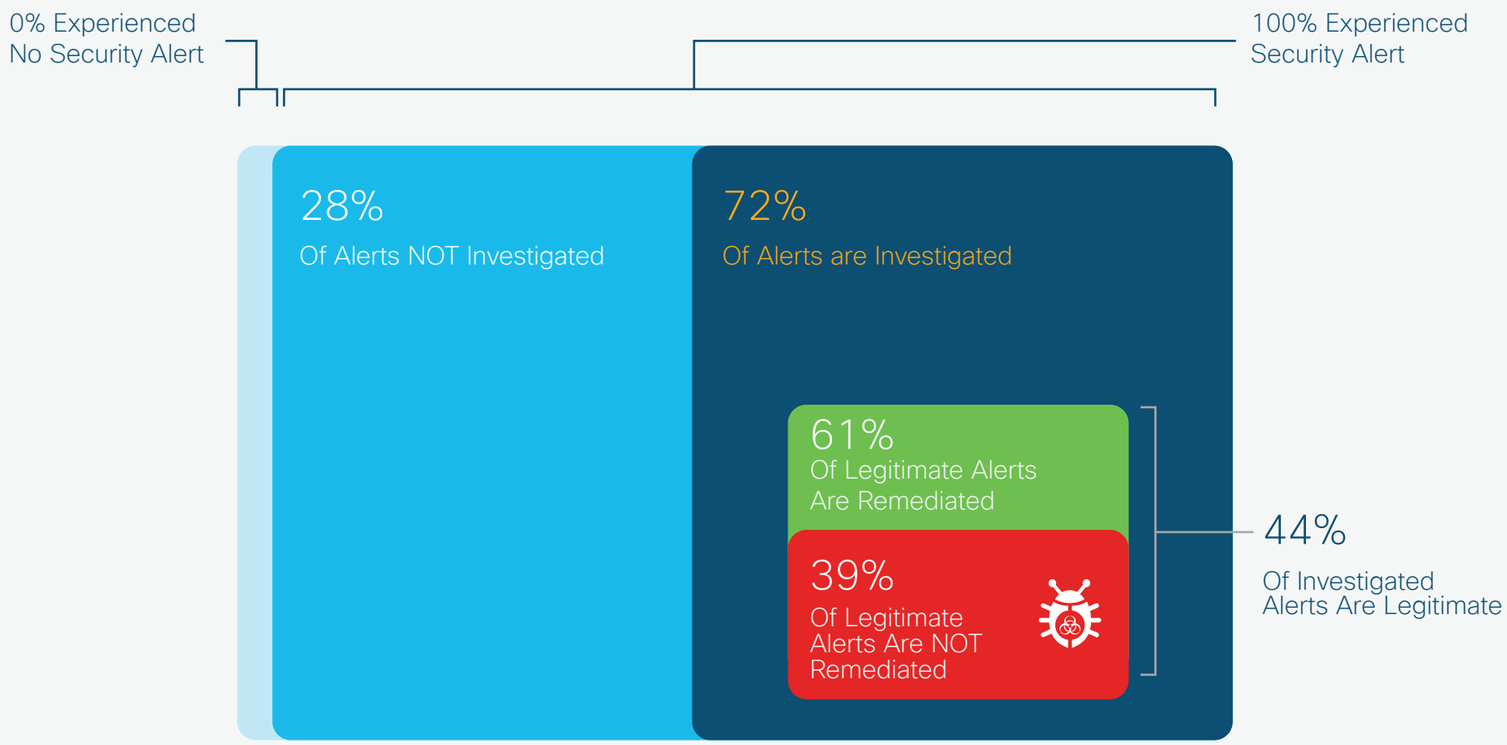
Security infrastructure plays a huge part in protecting an organization, but it is not the only thing that matters; governance is equally important. The Cisco 2017 Security Capabilities Benchmark Study found Indian organizations wanting in this area, prevented perhaps from following a good security discipline by legacy technology and lack of manpower and technical knowledge.

Indian organizations investigate 63 percent of security alerts – the global average is 56 percent – of which 39 percent turn out to be legitimate, on average. The organizations end up fixing 47 percent of legitimate alerts.

Government sector respondents said they investigated 72 percent of the alerts they received, and observed that a little less than half of them (44 percent) were genuine. They finally remediated 61 percent of these legitimate alerts.

Based on these responses, one can conclude that government organizations are much more diligent in investigating security issues than Indian organizations on average. For instance, they remediate almost twice the number of issues that financial services companies, which are also prone to cyber attack, do.

Figure 4. Percentage of Security Alerts That Are Not Investigated or Remediated in Government Sector



2016 (n=22)

Source: Cisco 2017 Security Capabilities Benchmark Study

The following hypothetical example helps in understanding the level of investigation and remediation of security alerts in Indian government entities:

If a government organization in India records 5,000 alerts every day:

- It investigates 3,600 alerts (72 percent) and ignores 1,400 (28 percent)
- Of the 3,600 alerts that are investigated, about 1,584 (44 percent) are found to be legitimate, while 2,016 (56 percent) are not
- Of the 1,584 legitimate alerts, the organization remediates 966 (61 percent) and does not remediate the remaining 618 (39 percent) alerts

While government organizations do better than others, they still let a substantial number of alerts go uninvestigated. Since it is almost impossible to investigate every threat manually, they should consider using automation and integrated security solutions to increase the breadth of coverage.

Until that happens, Indian government organizations will run the risk of being seriously impacted by a breach someday. This could, at a minimum, compromise operations or reputation, and in the worst case, threaten their very existence. In the global study, many respondents shared their concern about even minor security incidents negatively impacting their bottom-line. India's government establishments would do well to bear this in mind at all times.

Any lapse in vigilance could result in a breach, and place a huge burden of damage control on the security team. In addition, it could put the network out of action for a reasonably long time. When the survey respondents were asked about their most severe security breach in the past year, a surprising number reported facing lengthy outages. At 38 percent of Indian organizations, the outage lasted between 1 and 8 hours; in the government sector, this number was comparable at 36 percent. 32 percent of government organizations faced a longer outage lasting 9 to 16 hours.

Besides downtime, the impact on systems is a major point of concern in any breach. In the survey, 10 percent of government sector respondents said that their worst security breach in the past year impacted between 1 and 10 percent of their systems. For another 29 percent, it was worse, with anything between 11 and 30 percent of their organization's systems getting affected. At a very substantial 38 percent of organizations, the breach impacted more than half the systems.

Figure 5. Length and Extent of Outages Caused by Security Breaches in Government Sector

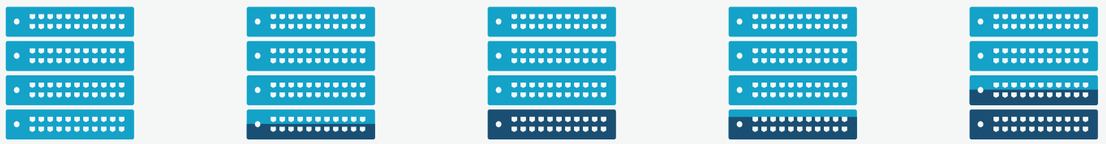
Organisations' Systems Down Time Due to Breach

2016 (n=22)

No Outage	Less Than 1 Hour	1–8 Hours	9–16 Hours	17–24 Hours	Over 24 Hours
5%	9%	36%	32%	0%	18%

Percentage of Systems Impacted Due to Breach

2016 (n=21)



No Impact	1–10% Impacted	11–30% Impacted	31–50% Impacted	Over 50% Impacted
0%	10%	29%	24%	38%

Source: Cisco 2017 Security Capabilities Benchmark Study

Impact: Breaches Cause More than Outage; Invite Public Scrutiny and Impact Business

The effects of breaches aren't limited to outages. Breaches also mean the loss of money, time, and reputation. Security teams who believe they will dodge this bullet are ignoring the reality of the data. As our study shows, almost two-thirds of Indian organizations have had to cope with public scrutiny following a security breach. Given the attackers' range of ability and tactics, the question isn't if a security breach will happen, but when.

Moving to India's government sector, 82 percent of organizations, compared to 62 percent in India overall, faced public scrutiny because of a breach. 17 percent of organizations said the breach was disclosed involuntarily, and made public by third parties. 44 percent of organizations disclosed the breach because of reporting or legal requirements, whereas 39 percent did so voluntarily.

When any entity makes the headlines for a security breach, it suffers the consequences long into the future. And because communication is now instantaneous, there are reactions from all over the world. Breaches can cause substantial damage to business organizations, but in the case of government establishments, the impact can be far worse, if one were to count the political and economic fallout of the incident and its effect on the citizens.

Hence government entities should be doubly careful about their security infrastructure. Hackers are continually becoming more capable and even more ambitious. Just because a government's systems have not been breached so far does not mean they are impregnable. When it comes to security, it is best to be proactive and err on the side of caution.

Figure 6. Percentage of Government Organizations Experiencing a Public Breach

82%

Had to Manage Public Scrutiny of a Security Breach
2016 (n=22)

How the Most Recent Breach Became Known Externally

(n=18)

Involuntarily Disclosed (Third-Party)

17%

Required Reporting (Regulatory/Legal)

44%

Voluntarily Disclosed

39%

Source: Cisco 2017 Security Capabilities Benchmark Study

Outages do more than disrupt the business rhythm; they can cause the loss of money, reputation and customers.

Worldwide, and also in India, respondents named operations as the area most likely to be affected by an outage. Government organizations too named operations first (41 percent), followed by legal engagements (36 percent), business partner relationships, intellectual property and regulatory scrutiny (32 percent each).

Indian government entities, especially the large ones, cannot afford an interruption in operations since they serve a large part of the country and its people with public services. Therefore those in charge of security should make sure their organization is well protected, and be ready with a recovery strategy in case there is a breach.

Figure 7. Functions Most Likely to Be Affected by a Public Breach in Government Sector

Source: Cisco Security Research

What kind of losses did organizations from the Indian government sector experience as a result of a security incident? Figure 8 shows that 50 percent of government organizations lost business opportunities, a bit higher than Indian organizations overall (43 percent).

9 percent of these organizations lost less than 20 percent of opportunity, and 64 percent lost opportunities that were between 20 and 39 percent. Compared to this, the loss experienced by Indian organizations overall was a little more spread out (35 percent lost less than 20 percent, 35 percent lost between 20 and 39 percent and 30 percent lost between 40 and 100 percent).

Figure 8. Percentage of Business Opportunity Lost at the Result of Attach in Government Sector

Source: Cisco 2017 Security Capabilities Benchmark Study

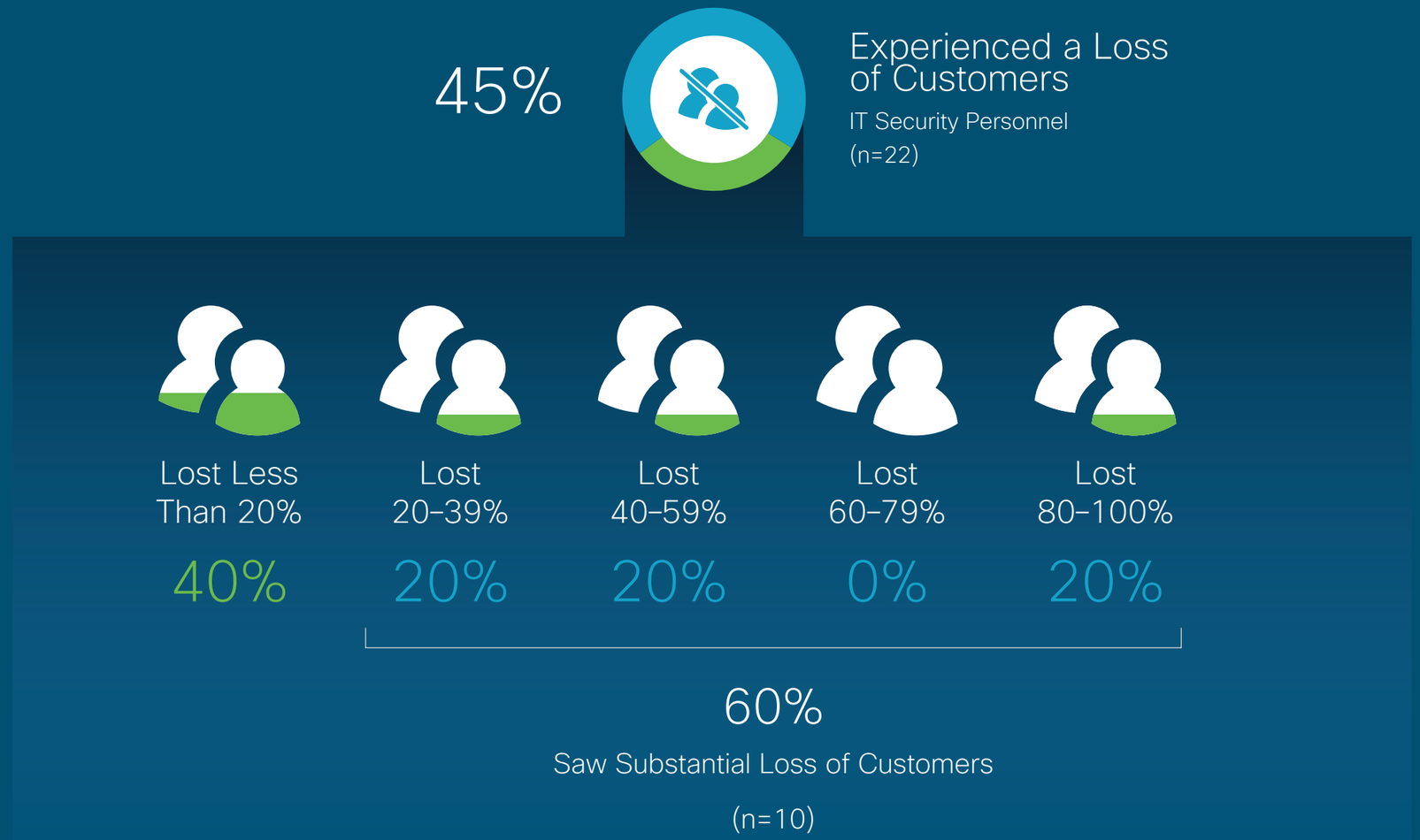
Slightly more than half, or 55 percent of organizations lost revenue due to a security attack. Of these organizations, 25 percent lost less than 20 percent of revenue, whereas 33 percent lost between 20 and 39 percent.

Figure 9. Percentage of Government Organizational Revenue Lost as the Result of an Attack

Source: Cisco 2017 Security Capabilities Benchmark Study

45 percent of Indian government organizations also lost customers when they had a security breach. Of these, the single biggest chunk – 40 percent – lost less than 20 percent of their customers, while another 20 percent lost between 20 and 39 percent of customers. This is almost identical to the situation of Indian organizations overall.

Figure 10. Percentage of Customers Lost by Government Organizations Due to Attacks



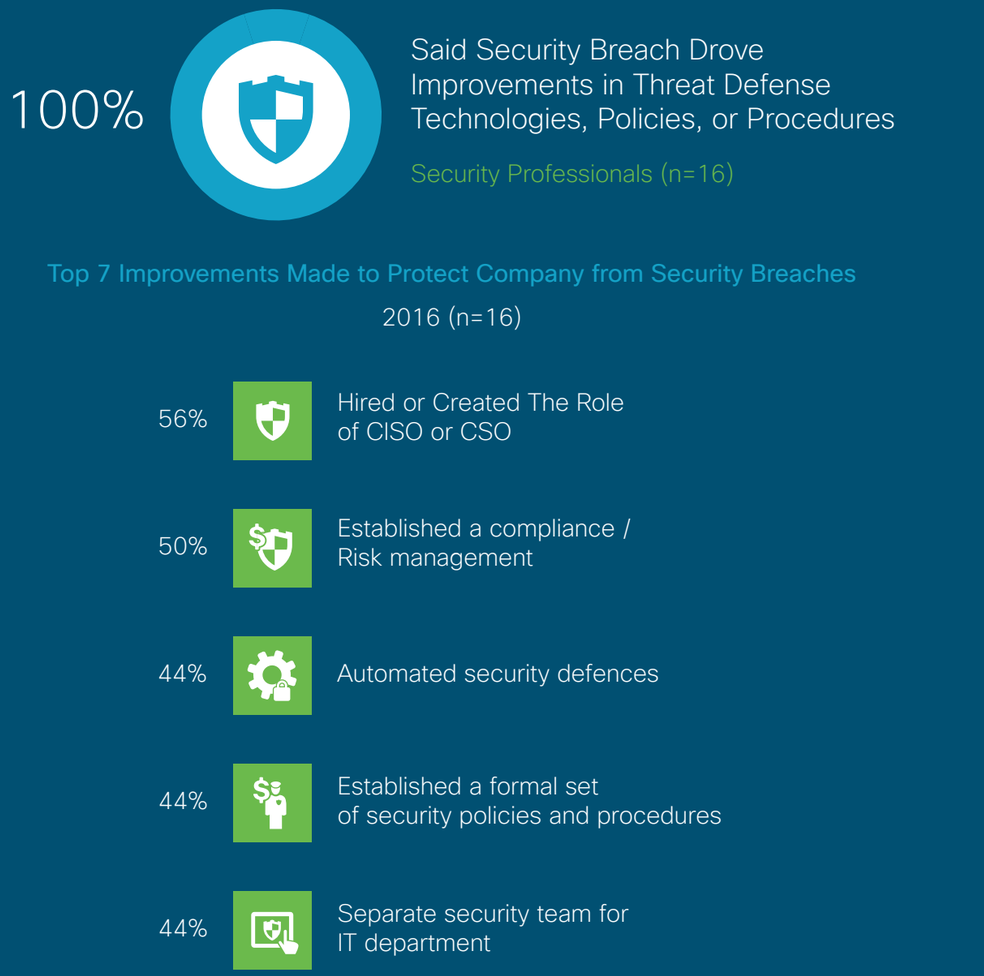
Source: Cisco 2017 Security Capabilities Benchmark Study

Outcomes: Scrutiny Drives Security in Government Organizations

Organizations hit hard by cyber attack also have to manage its fallout in the media. Although negative publicity has many undesirable consequences, it also forces the organization to tighten its defenses by strengthening the areas that are most vulnerable. These measures range from overhauling security infrastructure to building security awareness among staff to improving governance and regulatory compliance. One example of how Indian government organizations are responding to the rising threat around them is the Center of Excellence for Cyber Security, which is being set up by the Karnataka state government to ensure a swift and effective response to threats such as WannaCry. The Center will bring together academic institutions and industry experts from around the world so they can share their knowledge to drive improvements in cyber security.

As far as the government organizations in the survey are concerned, there is universal agreement that a breach, and the resulting public scrutiny, drives improvement in security measures. For the maximum number of respondents (56 percent), the improvement was the hiring or creation of the role of Chief Information Security Officer or Chief Security Officer. At 50 percent of organizations, a breach resulted in the establishment of a compliance / risk management office, whereas at 44 percent of organizations, it led to the automation of security defenses, formalization of security policies and procedures, and separation of the security team from the IT department.

Figure 11. How Security Breaches Drive Improvements in Government Sector



Source: Cisco Security Research

Increasingly, security is becoming everyone's business. This is only to be expected given that technology has pervaded every function, and that all types of users (and not just IT) are taking technology related decisions. With security becoming more and more important to organizational health and performance, most stakeholders are turning their attention to it. It is very important to reassure them that their organization is well protected.

In the study, 89 percent of security professionals in India expected scrutiny from clients and customers, 88 percent said it would come from business partners, and 87 percent believed it would come from regulators and executive leadership both. For government organizations, the most important source of scrutiny was watchdogs/ interest groups, named by 95 percent of respondents, which is quite understandable because they often come under fire from citizen groups and activist organizations. 91 percent of respondents said they expected scrutiny from regulators, business partners and clients/ customers. Surprisingly, the press was deemed the least important source of scrutiny (73 percent).

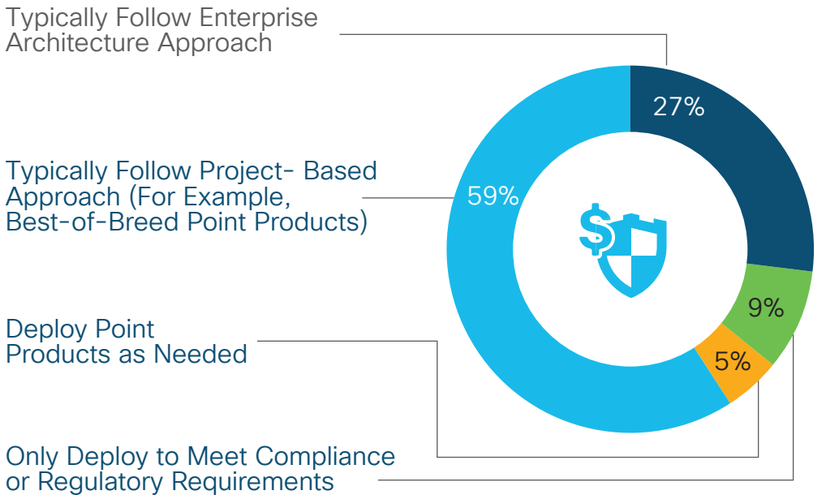
Figure 12. Sources of Increased Security in Government Sector

Source: Cisco 2017 Security Capabilities Benchmark Study

Figure 13. How Trust and Cost-Effectiveness Drive Security Decisions in Government Sector

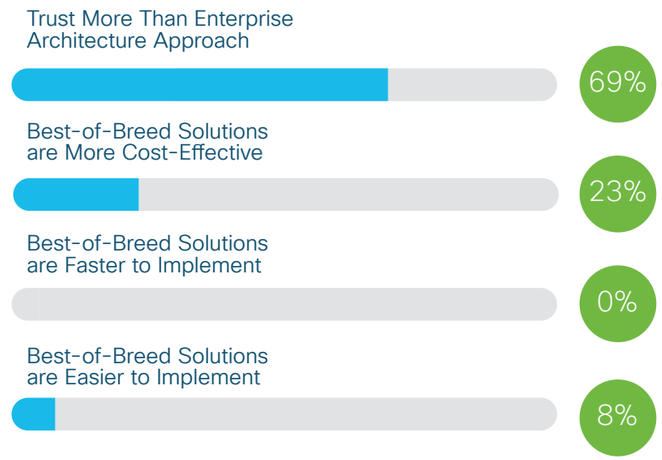
Security Threat Defense Solution Purchasing

IT Security Personnel (n=22)



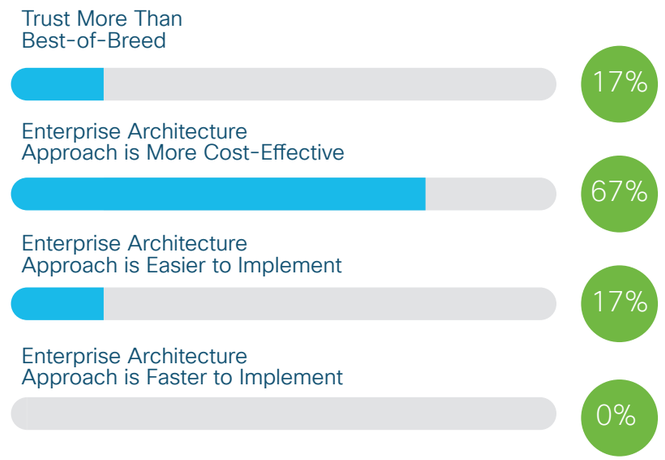
Reasons for Favoring a Best-of-Breed Approach

Organisation That Purchased Best-of-Breed Point Solutions



Reasons for Favoring an Enterprise Architecture Approach

Organisations That Typically Follow an Enterprise Architecture Approach



Trust Versus Cost: How do Indian GovernmentOrganizations Decide Security Purchases?

The Cisco 2017 Security Capabilities Benchmark Study showed that more security professionals in India preferred buying best-of-breed solutions to the enterprise architecture approach; globally, the choice was evenly split between the two.

As mentioned earlier, India's government establishments also favor point solutions and vendors, but use significantly more of each than the average Indian organization. How do they decide which solutions to buy? Is the decision influenced by an existing relationship with a trusted vendor, or based purely on commercial factors?

Since every security professional is in search for the best solution for the organization perhaps there is a case for examining the integrated architecture option. Decision makers need to weigh all these factors as well as practical aspects, such as ease and speed of implementation.

Coming back to the survey results, 59 percent of respondents from the government sector preferred best-of-breed security solutions, and 27 percent preferred an integrated architecture approach.

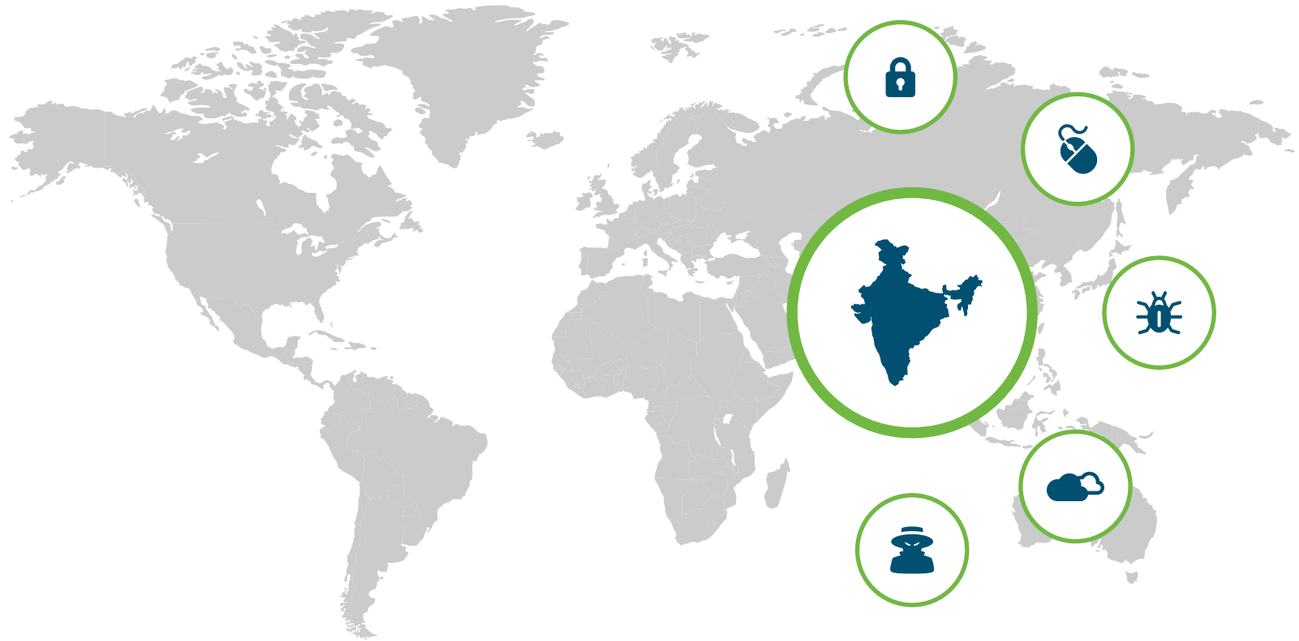
Their reason for choosing these approaches was consistent with the findings for Indian organizations overall. For those choosing best-of-breed solutions, it was trust (69 percent), whereas for those using an enterprise architecture approach, it was cost effectiveness (67 percent).

Since both approaches have distinct advantages, it is in an organization's best interest to use a combination that suits its needs. The integrated enterprise architecture approach gives the organization a holistic and detailed understanding of the overall defense to minimize the gaps open to attack, and leverages automation to enable faster detection. What's more, it is simple, scalable, and open enough to accommodate best-of-breed solutions where required.

Summary: What the Benchmark Study Reveals

The study clearly says that good security is not only about having the right tools and technologies; how Indian government organizations put them to work is very important. Currently, they face several constraints, including a lack of knowledge about advanced security processes and technology, and a “cultural” resistance to investing in unproven solutions that prevent them from leveraging their security infrastructure to the fullest. These barriers must be dismantled at the earliest to clear the path to adoption.

That being said, even the best security provisions are breached sometimes. Organizations cannot afford to be complacent, and should remain ever watchful for threats. Even organizational constraints cannot be totally eliminated. Security professionals simply need to accept this and do their best to constantly update their knowledge about advanced security processes and technology to adopt the same in their organizations.



Here, they will need the backing of their leaders to build a supportive culture and attitude towards cyber security throughout the organization. Security departments in Indian government organizations are grappling with a maze of vendors and point products, whose incompatibility is also an impediment to security. They can mitigate that challenge by using simple, effective security tools and an integrated architecture approach.

About Cisco

Cisco is building truly effective security solutions that are integrated, automated, open and simple to use. Drawing unparalleled network presence as well as the industry's broadest and deepest technology and talent. Cisco delivers ultimate visibility and responsiveness to detect more threats and remediate them faster. Talos, industry-leading team of security intelligence and research experts who regularly share analysis of threats and provide Cisco customers the tools to help protect against them. By calling on Cisco Security, companies are poised to securely take advantage of new world of digital business opportunities. For more details, visit https://www.cisco.com/c/en_in/products/security/index.html