Cisco 2017 Security Capabilities Benchmark Study

India Findings for Financial Services

India Findings for Financial Services

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.

This report presents the findings and analysis for Indian Financial Services organizations.

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 51 leading financial services respondents from India.

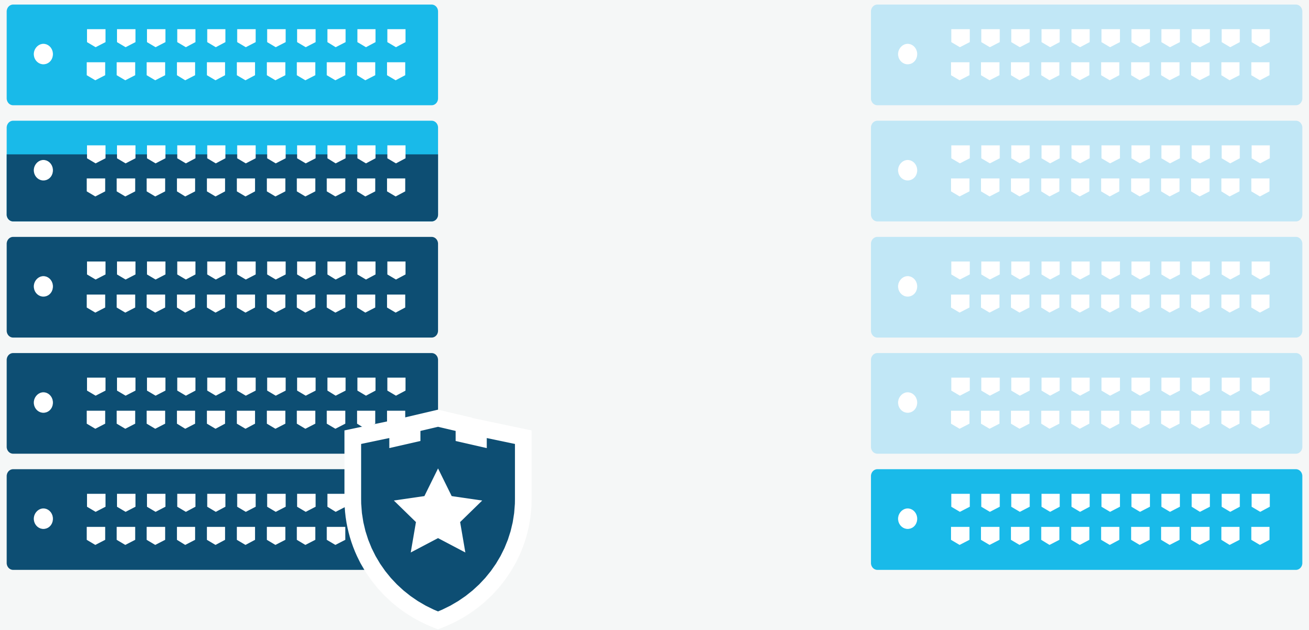
As Digital India marches on, aided by the growth of mobile and Internet technologies, consumer trends, and a push from the Government, it also faces a rising cybersecurity threat. Therefore, it is imperative that Indian enterprises, and financial institutions in particular, include a sound security strategy in their digitization agenda.

The Cisco 2017 Security Capabilities Benchmark Study found that the security provision at most Indian enterprises exists as a complex maze of vendors and outdated security products, which barely communicate with each other. While the situation is marginally better in financial services organizations, it is grave enough to create a hindrance to security adoption.
Clearly, this is not an optimal situation for Indian financial services organizations, which end up spending far too much money and effort on a security environment that is not fully effective. Banks and insurance companies caught in a legacy snarl should be looking at upgrading to 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

The survey found that despite rising threat, Indian organizations were very confident about their security technology. In 2016, 69 percent of CISOs and security operations professionals in India – significantly higher than the global figure, which stood at 58 percent – said that their security infrastructure is very up to date and is constantly upgraded with the best technologies available. Indian financial services organizations are even more upbeat, with 76 percent agreeing with this statement, and another 20 percent saying that they replace or upgrade their security technologies regularly even though they do not have the latest tools. (Figure 1)

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



Described as Very Up to Date

Best Technologies Available

76%

Described as Replaced/Upgraded on Regular Cadence

Not Equipped with Latest and Greatest Tools

20%

2016 (n=51)

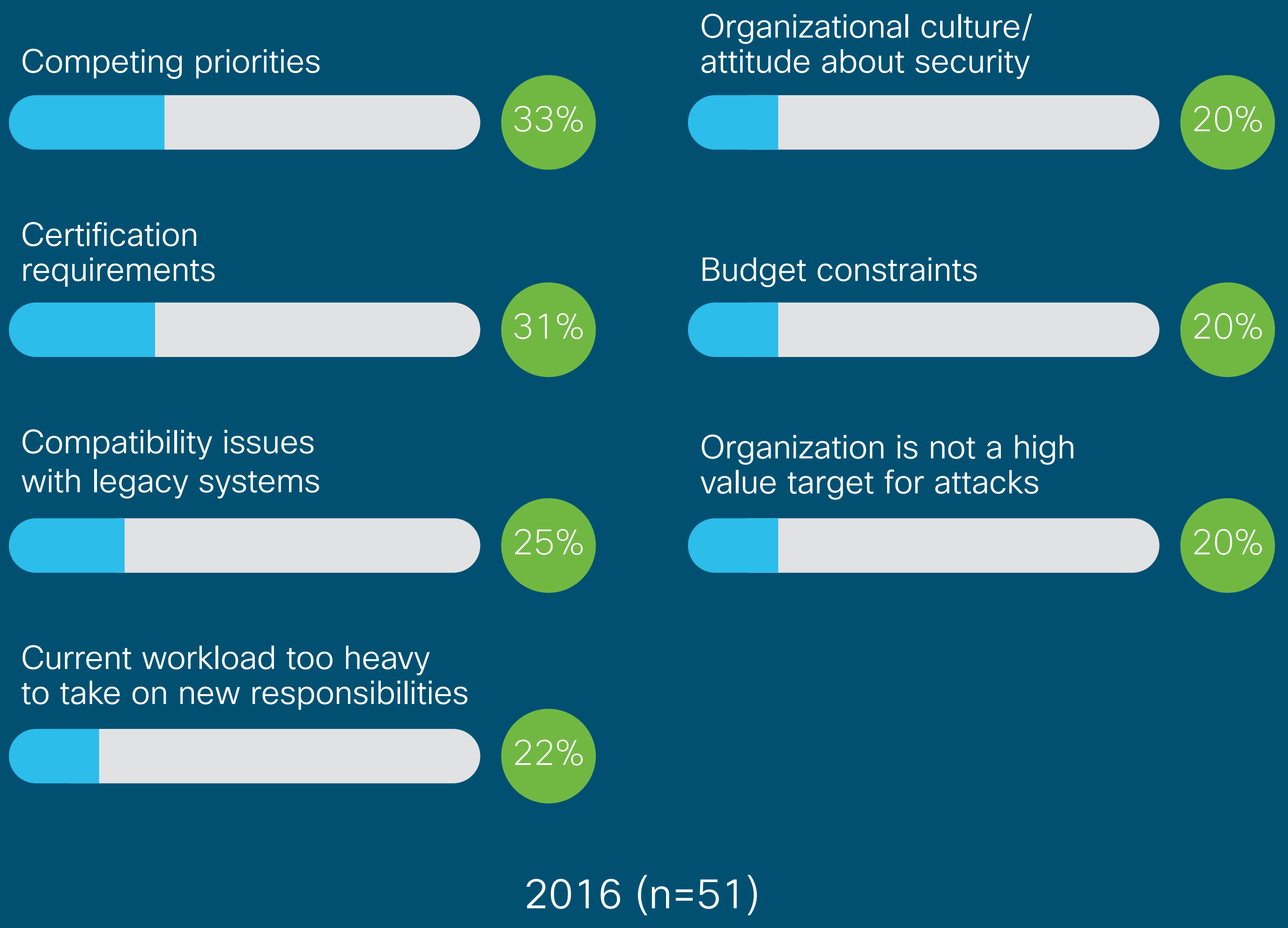
Source: Cisco 2017 Security Capabilities Benchmark Study

Constraints: Competing Priorities, Certification Requirements and Legacy Technology Hamper Organizations from Adopting Security Measures

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. For Indian organizations overall, the biggest barrier to security is organizational culture and attitude to security, closely followed by compatibility issues with legacy systems.

The situation is somewhat different for financial services where competing priorities and certification requirements pose the biggest barriers to security adoption. Lack of compatibility with legacy systems is the third biggest obstacle, and is followed by the organizations' heavy workload, which makes it difficult for them to take up new responsibilities. Budgetary constraints is in joint 5th place along with culture and attitude to security and a somewhat dangerous assumption that the organization is not a top target of attack. In 2016, 33 percent of security professionals in the Indian financial services industry said that competing priorities hampered them from adopting the latest security technology and processes. Coming on top of a considerable regulatory compliance burden, the certification requirements of advanced security solutions also deter financial services companies from embracing them: 31 percent of respondents said that this was a big problem. 25 percent of financial services respondents blamed incompatible legacy systems (compared to 28 percent in India overall) for not being able to implement security technologies and policies the way they should. (Figure 2)

Figure 2. Biggest Obstacles to Security



SHARE

Source: Cisco 2017 Security Capabilities Benchmark Study

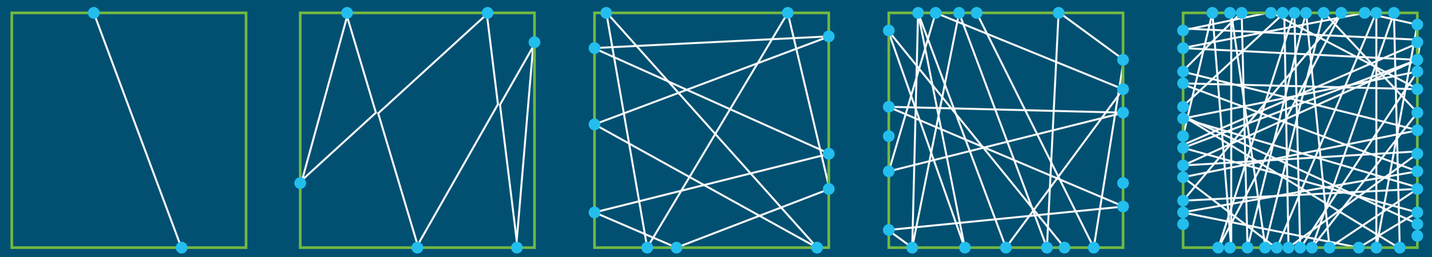
Ironically, too many point solutions can increase an organization's vulnerability to attack if they don't communicate and integrate with each other. Unfortunately, most security professionals in India, like their counterparts in other countries, have a tendency to juggle products from many vendors. This opens up gaps in time and space that cybercriminals can exploit, and prevents organizations from presenting a seamless defense to attack.

56 percent of Indian financial services companies use between 1 and 5 vendors, and 53 percent use between 1 and 5 products. (Figure 3) Even so, they use fewer vendors and products compared to other businesses in the country, where 56 percent of organizations use 6 or more vendors and 69 percent of organizations use 6 or more security products.

Figure 3. Number of Security Vendors and Products Used by Financial Services Organizations

Number of Security Vendors in Security Environment

2016 (n=51), Graphic Rounded to Nearest Whole Number

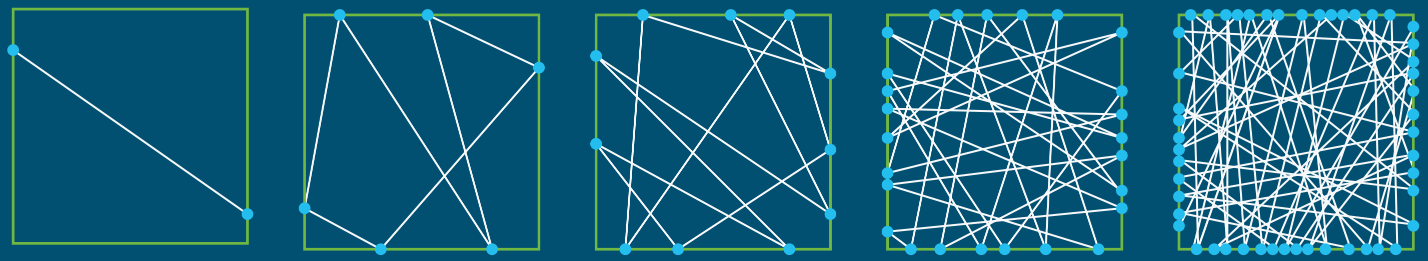


1–5 Vendors	6–10 Vendors	11–20 Vendors	21–50 Vendors	Over 50 Vendors
56%	8%	26%	8%	2%

44% Use more than 5 Vendors

Number of Security Products in Security Environment

2016 (n=201), Graphic Rounded to Nearest Whole Number



1–5 Products	6–10 Products	11–25 Products	26–50 Products	Over 50 Products
53%	8%	14%	14%	12%

47% Use More Than 5 Products

Source: Cisco 2017 Security Capabilities Benchmark Study

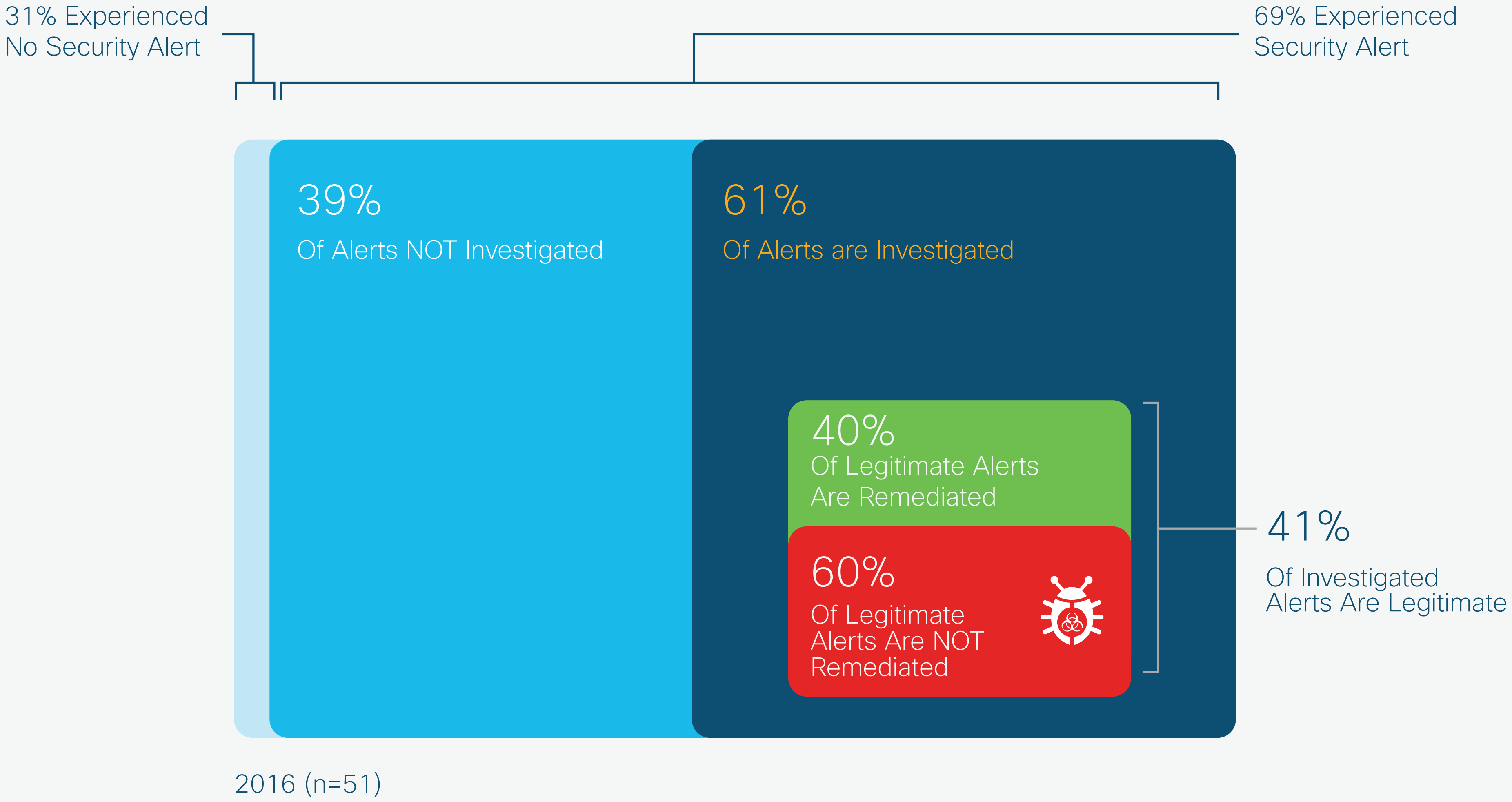
A cause for concern is that around the world, including in India, the presence of good security infrastructure does not automatically mean good governance. Incompatible legacy solutions, inadequate staff and a lack of knowledge about the latest advances in security processes are likely causes for this.

The Cisco 2017 Security Capabilities Benchmark Study shows that globally, 56 percent of security alerts are investigated, of which 28 percent are found legitimate on average. Only 46 percent of legitimate alerts are remediated. Indian organizations do marginally better by investigating 63 percent of alerts, of which 39 percent turn out to be legitimate. Finally, they fix only 47 percent of legitimate alerts.

Indian financial sector organizations fare slightly worse than this: they investigate about 61 percent of alerts received, and find 41 percent of investigated alerts to be legitimate on average. However, they remediate only 40 percent of legitimate alerts, which is significantly lower than the overall India and global numbers.

This leads one to ask whether Indian banks and insurance companies take the cybersecurity threat lightly – recall that quite a few believe they are not a prime target – or are unable to overcome the barriers that stand between them and a robust security environment.

Figure 4. Percentages of Security Alerts That Are Not Investigated or Remediated



Source: Cisco 2017 Security Capabilities Benchmark Study

The following hypothetical example illustrates the seriousness of the issue.

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

- It investigates 3,050 alerts (61 percent) and ignores 1,950 (39 percent).
- Of the 3,050 alerts that are investigated, about 1,251 (41 percent) are found to be legitimate, while 1,799 (59 percent) are not.
- Of the 1,251 legitimate alerts, the organization remediates only 500 (40 percent) and does not remediate the remaining 751 (60 percent) alerts.

It is worrying that approximately 2 out of 5 security alerts go uninvestigated in Indian banks and insurance firms. They must examine the uninvestigated alerts to make sure that no serious threats, such as a ransomware attack for instance, slip through the cracks. While it is true that security teams cannot manually investigate each and every one of the huge number of threats that arise everyday, with the help of automation and properly integrated security solutions, they can definitely cover a greater area of the threat landscape.

The fact that Indian financial services organizations ignore so many threats on a daily basis creates doubts about their ability to sustain in the long term. For instance, could these uninvestigated threats snowball into a problem that impacts business performance, customer satisfaction, or corporate reputation? Many of the respondents in the global study felt that even small network outages or minor security breaches could make a long-term impact on the company’s bottom line. Indian organizations should learn from this and view even seemingly minor incidents with seriousness.

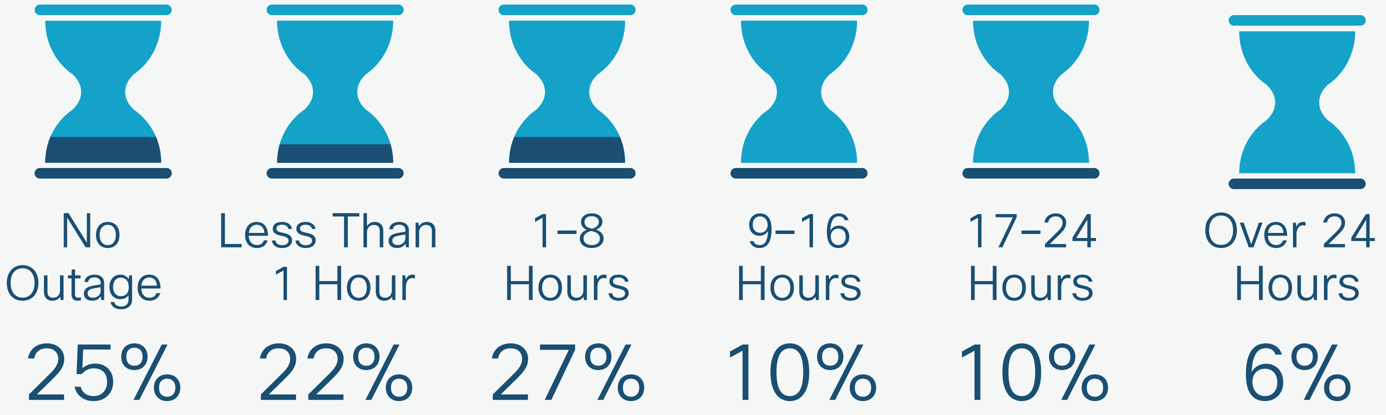
Failure to do so could result in a breach, putting untold stress on the security team, which is tasked with mitigating the damage. Our study shows that network outages can last quite long. In the case of their most severe security breach in the past year, systems were down for between 1 and 8 hours at 27 percent of Indian financial services organizations, substantially lower than the 38 percent of Indian organizations overall suffering the same fate. 10 percent of outages in financial services companies lasted 9 to 16 hours and a similar proportion of outages carried on for 17 to 24 hours. (Figure 5)

The severity of any breach is also felt in terms of the number of systems that are impacted. In the survey, 24 percent of financial services respondents said that their worst security breach in the past year impacted between 1 and 10 percent of their systems. For another 24 percent, it was worse, with anything between 11 and 30 percent of their organization's systems getting affected. (Figure 5)

Figure 5. Organizations' Systems Down Time Due to Breach

Organisations' Systems Down Time Due to Breach

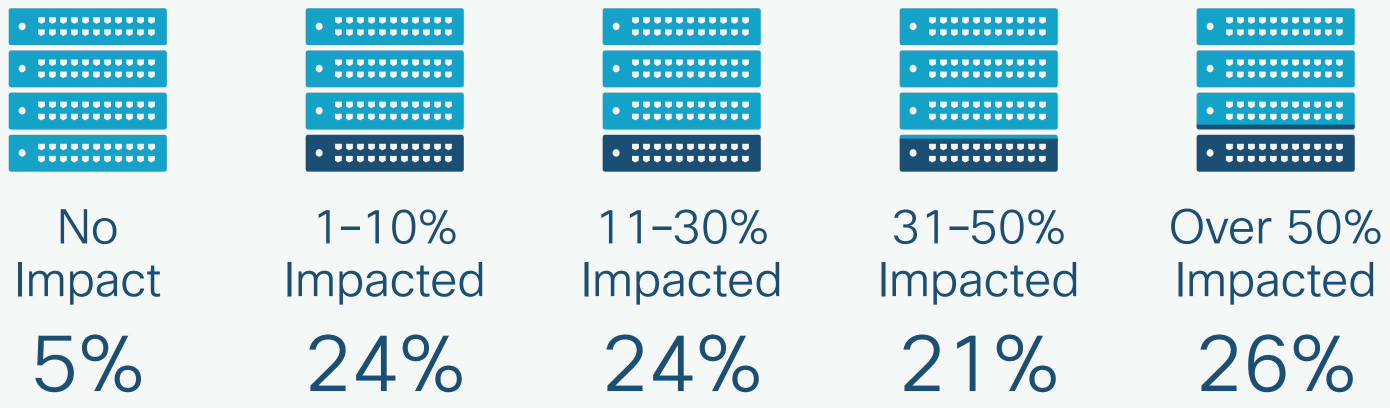
2016 (n=51)



No Outage	Less Than 1 Hour	1–8 Hours	9–16 Hours	17–24 Hours	Over 24 Hours
25%	22%	27%	10%	10%	6%

Percentage of Systems Impacted Due to Breach

2016 (n=38)



No Impact	1–10% Impacted	11–30% Impacted	31–50% Impacted	Over 50% Impacted
5%	24%	24%	21%	26%

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 the Indian financial services sector, 49 percent of organizations, compared to 62 percent in India overall, faced public scrutiny because of a breach. 44 percent of organizations said the breach was disclosed involuntarily, and made public by third parties. 16 percent of organizations disclosed the breach because of reporting or legal requirements, whereas 44 percent did so voluntarily. (Figure 6)

No company wants negative publicity. Unfortunately, with the increase in the number of cyber attacks, most organizations run the risk of being in the news for a breached security system. And because communication is now instantaneous, it doesn't take long for the news to travel around the world, causing untold damage in its wake.

This is all the more reason why organizations should never cease to be watchful about their security systems. As the recent WannaCry and Petya ransomware attacks show, cybercrime is continually evolving in capability and ambition. Just because a company has escaped attack until now does not mean it will be safe forever. It is better to be proactive in defense rather than be forced by untoward events to increase reinforcements.

Figure 6. Percentage of Organizations Experiencing a Public Breach

49% Had to Manage Public Scrutiny of a Security Breach
2016 (n=51)

How the Most Recent Breach Became Known Externally

(n=25)

Involuntarily Disclosed (Third-Party)	Required Reporting (Regulatory/Legal)	Voluntarily Disclosed
44%	16%	44%

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. (Figure 7)

Worldwide, and also in India, respondents named operations as the area most likely to be affected. However, 41 percent of Indian financial services respondents felt that finances and brand reputation would suffer the greatest impact if there were an outage.

Operations came next, named by 31 percent of respondents, followed by regulatory scrutiny (named by 29 percent), and customer retention (25 percent).

The Indian financial services market is extremely competitive and slippage in any area can drag an organization down hard. Security professionals at Indian banks and insurance companies should fortify their organizations' defenses against possible attack and also have a plan to get the business back on its feet quickly, should the worst happen.

No organization that plans to grow and achieve success wants to be in a position of having critical departments affected by security breaches. Security professionals should view the survey results with an eye toward their own organizations, and ask themselves: If my organization suffers this kind of loss from a breach, what happens to the business down the road?

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

Brand Reputation	41%
Finances	41%
Operations	31%
Regulatory Scrutiny	29%
Customer Retention	25%
Supplier Relationships	18%
Legal Engagements	16%
Intellectual Property	16%
Business Partner Relationships	10%
No Security Breach	2%

Source: Cisco 2017 Security Capabilities Benchmark Study

Security breaches also cause significant opportunity loss. As shown in Figure 8, 33 percent of security professionals in Indian financial services companies said their organizations lost business opportunities because of attacks in 2016, somewhat less than the corresponding figure for Indian organizations overall, which was 43 percent. Of the organizations that lost business opportunity, 18 percent said the loss was less than 20 percent, 18 percent said it was between 20 and 39 percent, 53 percent said it was somewhere between 40 and 59 percent, while 12 percent suffered a loss greater than 60 percent. The sector appears to have been impacted more than others, because overall, Indian organizations reported more losses of a lower order, that is, up to 39 percent, whereas the bulk of financial services organizations' losses were in the 40 to 59 percent range.

Figure 8. Percentage of Business Opportunity Lost as the Result of an Attack

33%

Experienced a Loss of Opportunity

IT Security Personnel
(n=51)

Lost Less Than 20%	Lost 20–39%	Lost 40–59%	Lost 60–79%	Lost 80–100%
18%	18%	53%	6%	6%

83%

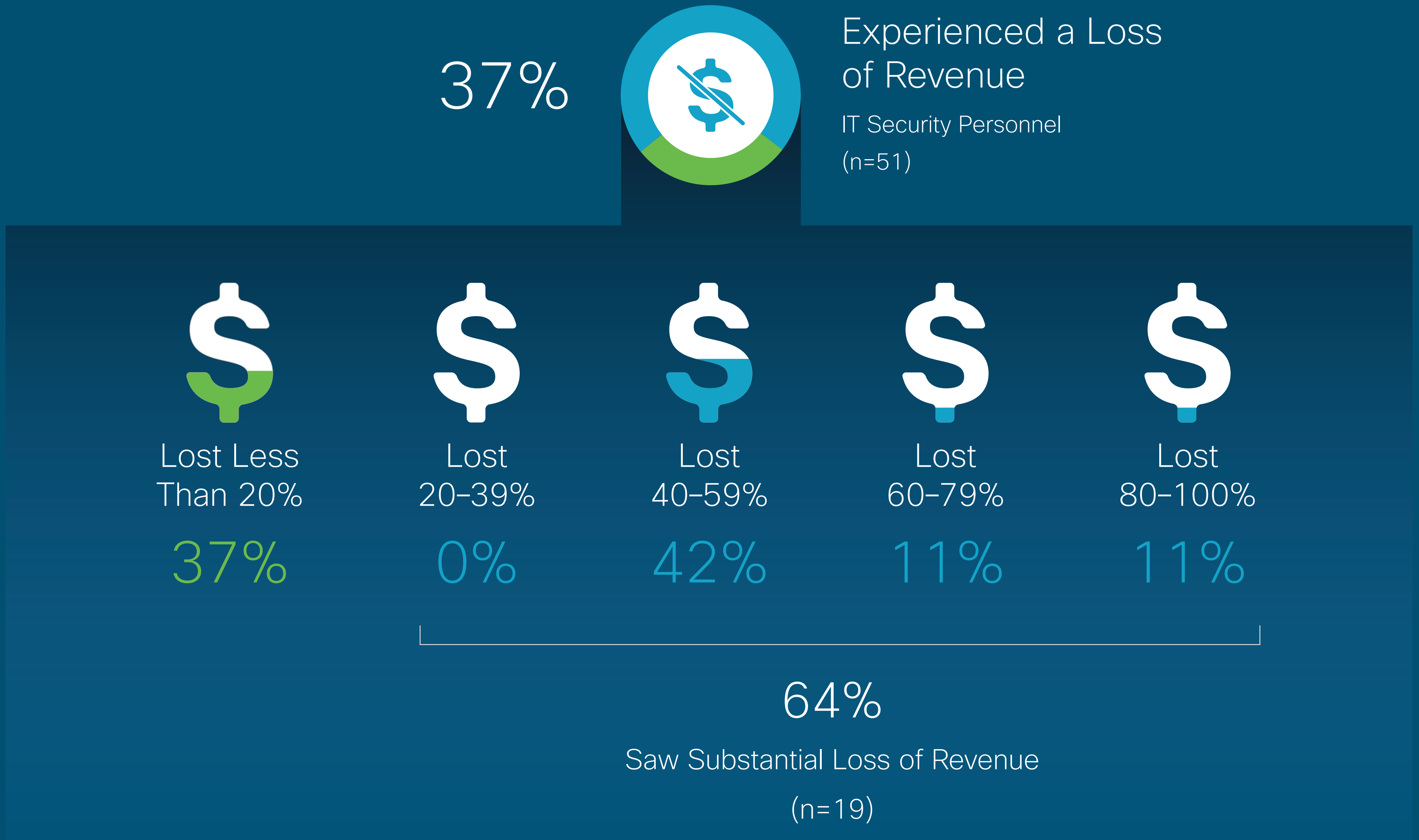
Saw Substantial Loss of Opportunity

(n=17)

Source: Cisco 2017 Security Capabilities Benchmark Study

37 percent of financial services companies reported loss of revenue due to an attack on security. Of these organizations, 37 percent lost less than 20 percent of revenue, whereas 42 percent lost between 40 and 59 percent. (Figure 9)

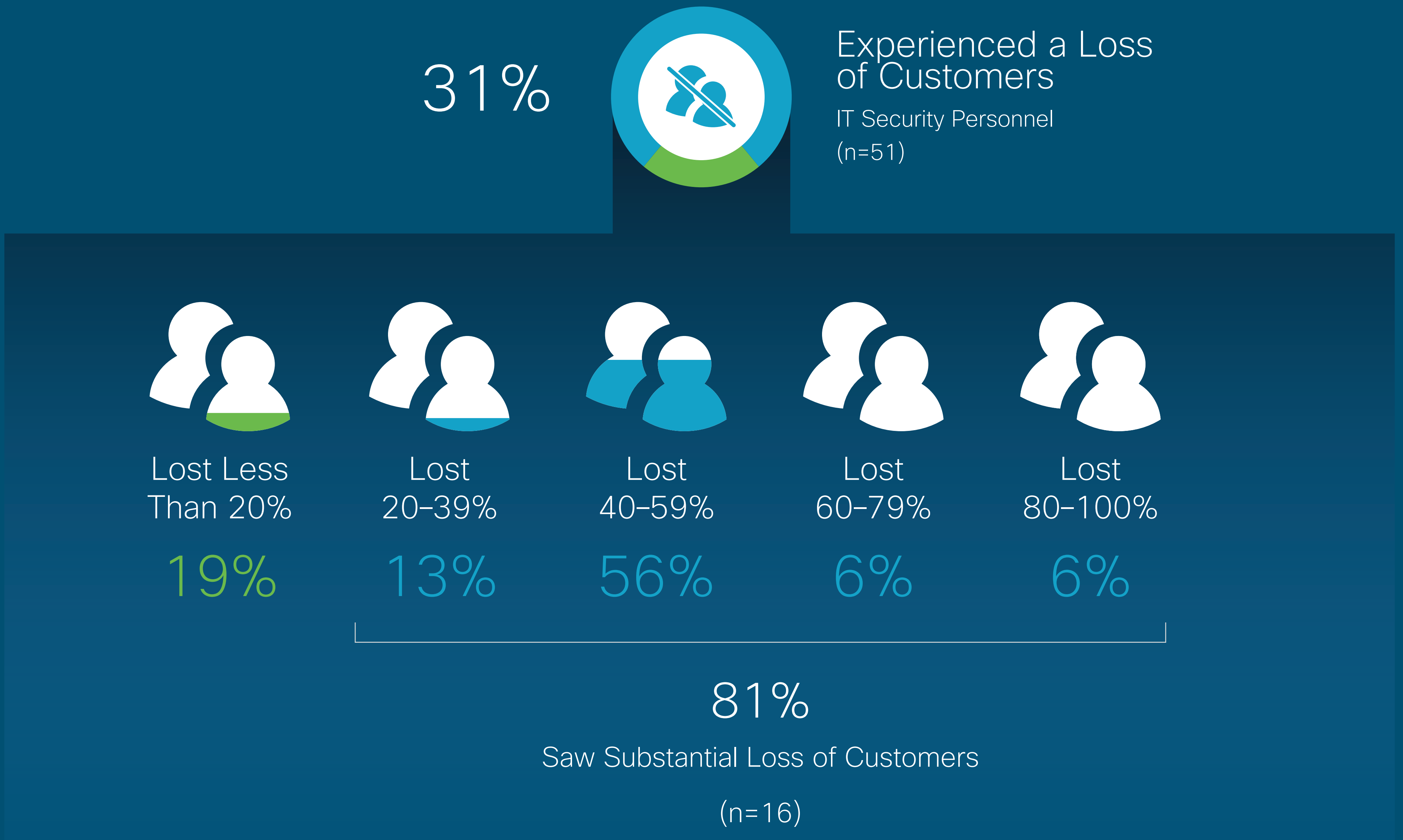
Figure 9. Percentage of Organizational Revenue Lost as the Result of an Attack



Source: Cisco 2017 Security Capabilities Benchmark Study

Security breaches also erode organizations' ability to win or retain customers. Figure 10 says that 31 percent of financial services organizations lost customers on this account. 19 percent of them lost less than 20 percent of customers, 13 percent lost 20 to 39 percent of customers, and the bulk, 56 percent to be precise, lost a substantial 40 to 59 percent of customers.

Figure 10. Percentage of Customers Lost by Companies Due to Attacks



31% Experienced a Loss of Customers

IT Security Personnel (n=51)

Lost Less Than 20%	Lost 20–39%	Lost 40–59%	Lost 60–79%	Lost 80–100%
19%	13%	56%	6%	6%

81%

Saw Substantial Loss of Customers

(n=16)

Source: Cisco 2017 Security Capabilities Benchmark Study

Outcomes: Greater Scrutiny Means Better Security

From inviting public scrutiny to denting revenue, a security breach can hurt an organization in many ways. No company, however robust its security systems, can claim to be totally immune to attack. It is therefore advisable to stay alert, periodically review preparedness to withstand attack, and bolster defenses by focusing attention and resources on the areas that are most vulnerable.

Even well secured organizations are breached from time to time. The best thing to do is to understand and fix what went wrong and then move on with business as usual. The bulk of Indian organizations display such resilience: in our India study, 94 percent of organizations that had managed public scrutiny due to a security breach said it drove improvements, ranging from increasing security awareness training among employees to strengthening enforcement of data protection laws and regulations. In the case of financial services organizations, 88 percent of those facing public scrutiny said the breach helped to drive improvements in security policies, procedures or technologies. Of those who faced public scrutiny, 56 percent said they increased security awareness training among employees, while 48 percent said they invested more in training security staff following the breach. (Figure 11)

Figure 11. How Security Breaches Drive Improvements

88%

Said Security Breach Drove Improvements in Threat Defense Technologies, Policies, or Procedures

Security Professionals (n=25)

Top 7 Improvements Made to Protect Company from Security Breaches

2016 (n=25)	
56%	Increased Security Awareness Training Among Employees
48%	Increased Investment in Training of Security Staff
36%	Increased Enforcement of Data Protection Laws & Regulations
36%	Formed a Team Specializing In Security
36%	Separated Security Team from IT Department
36%	Automated Security Defenses
36%	Increased Investment in Security Defense Technologies or Solutions

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 business users often purchase technology, spending from their own technology budgets. With security becoming more and more important to organizational health and performance, most stakeholders are turning their attention to it. Organizations need to reassure them on this count.

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. Financial services organizations thought differently, and claimed that regulators and executive leadership would be the biggest sources of scrutiny (named by 96 percent in both cases). This is understandable given that banks and insurance companies are highly regulated. Watchdog/ interest groups (94 percent), investors (92 percent) and business partners (90 percent) were next in line as important sources of scrutiny. (Figure 12)

Figure 12. Sources of Increased Scrutiny

Regulators	96%
Executive Leadership	96%
Watchdog and Interest Groups	94%
Investors	92%
Business Partners	90%
Clients and Customers	88%
Employees	86%
Insurance Companies	82%
Press	82%

2016 (n=51)

Source: Cisco 2017 Security Capabilities Benchmark Study

Trust Versus Cost: How do Indian Financial Services Organizations Decide Security Purchases?

The decision of which security solution strategy to deploy can make a big difference to the outcome. Naturally, all security professionals want the best for their organization, but what that is, isn't always clear. Should they go with a best-of-breed solution from an existing, trusted vendor? Or should they decide in favor of an integrated architecture option, which might be more cost effective? Apart from these considerations, ease of implementation is also a significant factor in the decision.

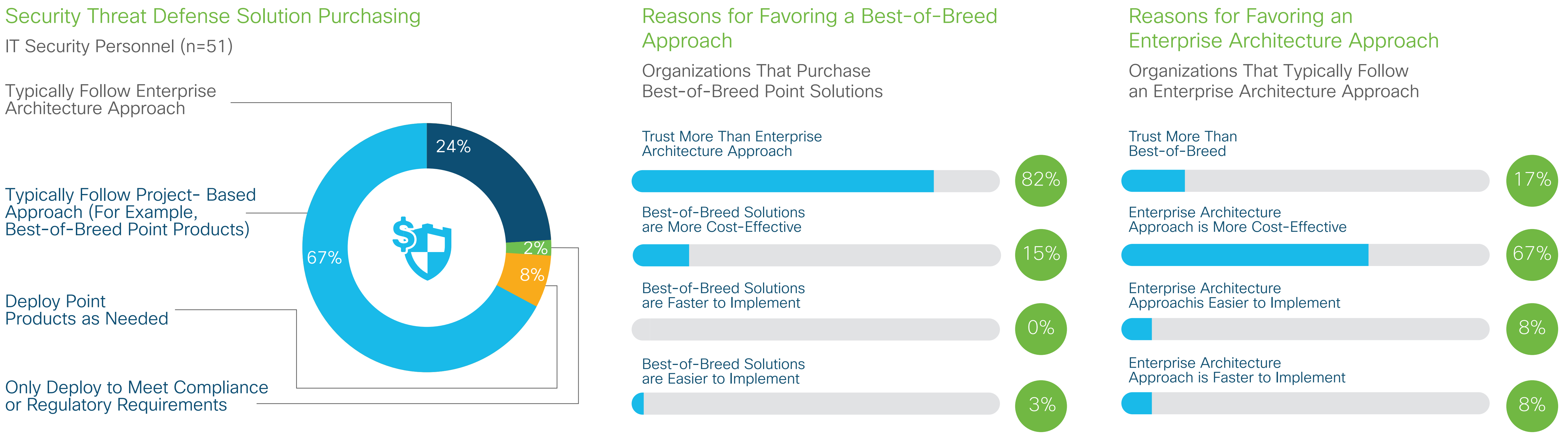
The Cisco 2017 Security Capabilities Benchmark Study showed that more security professionals in India preferred buying best-of-breed solutions to the enterprise architecture approach; globally, the choice was evenly split between the two.

Indian financial services organizations also preferred the best of breed approach, with 67 percent voting in its favor. The enterprise architecture approach was the choice of 24 percent of companies. 8 percent said they deployed point products as needed.

Their reason for choosing these approaches was consistent with the findings for Indian organizations overall. For those choosing best-of-breed solutions, it was overwhelmingly trust (82 percent), whereas for those using an enterprise architecture approach, it was cost effectiveness (67 percent).

The fact is that organizations need to deploy both options in the right measure to maximize benefit as well as make security simpler and more effective. The integrated enterprise architecture approach helps security professionals understand what is happening at every stage of defense, to reduce the operational space open to attack. It is simple, scalable, and open enough to accommodate best-of-breed solutions where required. Last but not least, the enterprise architecture approach is automated to enable faster threat detection.

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



Security Threat Defense Solution Purchasing

IT Security Personnel (n=51)

Reasons for Favoring a Best-of-Breed Approach

Organizations That Purchase Best-of-Breed Point Solutions

Reasons for Favoring an Enterprise Architecture Approach

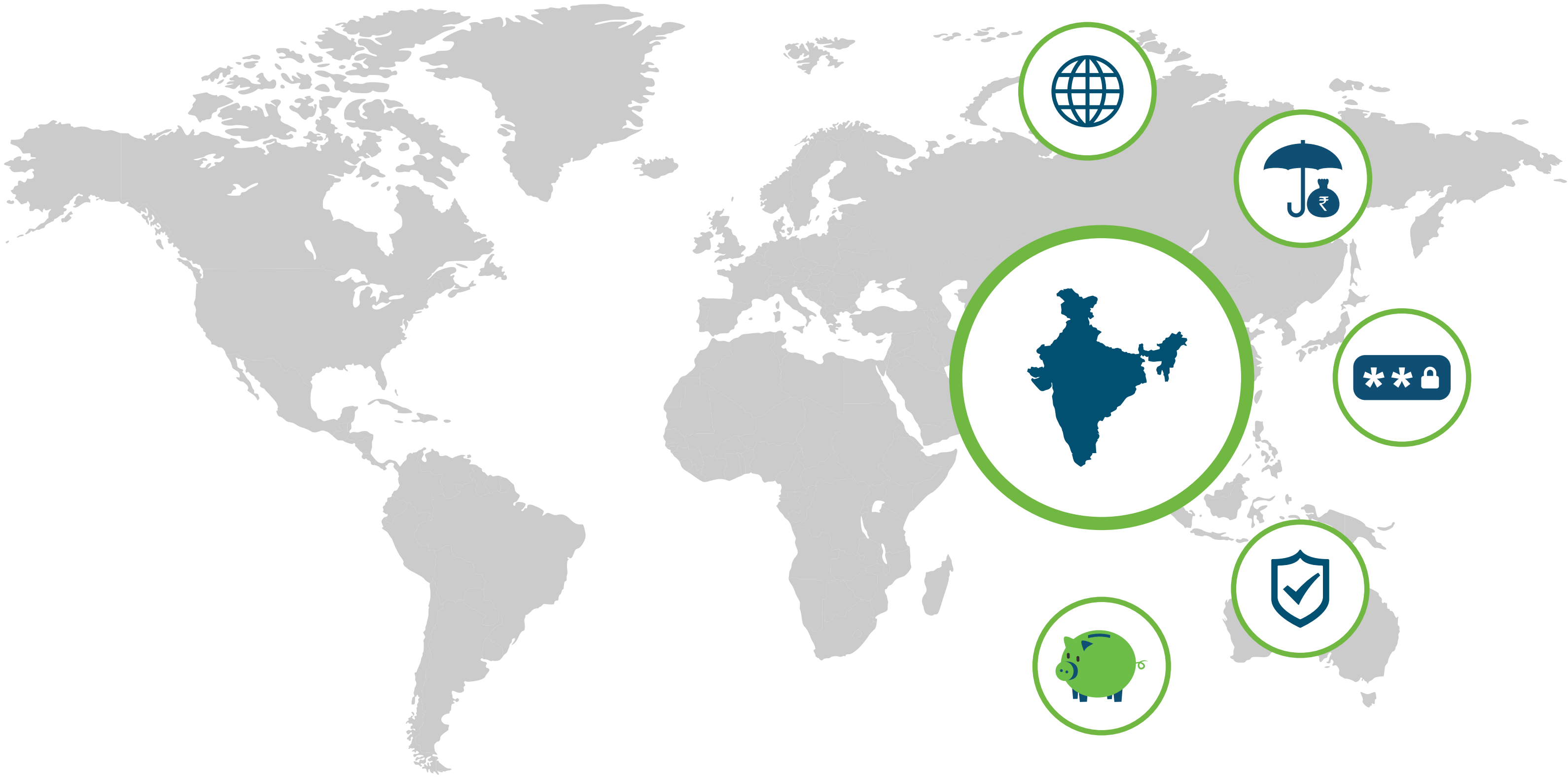
Organizations That Typically Follow an Enterprise Architecture Approach

Summary: What the Benchmark Study Reveals

The study clearly says that good security is not only about having the right tools and technologies; how organizations put them to work is very important. Indian financial services companies face several constraints, such as the need to balance competing priorities and manage incompatible legacy solutions, that prevent them from leveraging their security infrastructure to the fullest.

By hindering security adoption, these constraints increase organizations' vulnerability to attack. That is something to be avoided, and security professionals should act quickly to strengthen processes and protocols.

But 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 cybersecurity throughout the organization. Security departments in Indian financial services organizations are also grappling with multiple vendors and a number of legacy products, whose incompatibility is one of the biggest barriers 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