Cisco 2017 Security Capabilities Benchmark Study

India Manufacturing Sector Findings

cisco

India Manufacturing Sector Findings

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 23 respondents from the Indian Manufacturing Sector.

A number of digital technologies, including Artificial Intelligence, Industrial Internet of Things, Cloud, Additive Manufacturing, Augmented Reality and Analytics, are taking the manufacturing industry to Industry 4.0, or the fourth industrial revolution. This is giving rise to smart factories and cyber-physical manufacturing systems, which network extensively with each other and also communicate with human beings over the Internet. At the same time, it is also increasing the exposure of manufacturing organizations to cyber risk. In the Cisco 2017 Security Capabilities Benchmark Study, almost 40 percent of manufacturing organizations worldwide said that targeted attacks and advanced persistent threats were high security risks to their organizations and 28 percent claimed to have lost revenue due to cyber attack in the past year.

What is the situation in India? As the Indian manufacturing industry digitizes rapidly, it needs to watch out and protect itself against the inevitable menace of cyber attack, which can not only dent reputation and revenue, but also sabotage the safety of systems, damage the environment, and risk worker health and safety.

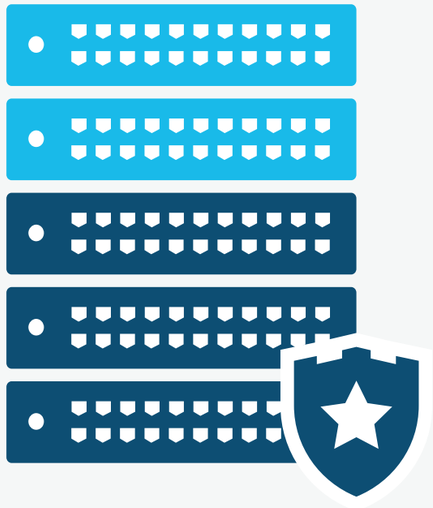
At present, the sector has made some provision for security. However, the infrastructure is more often than not a complex maze of vendors and solutions that rarely integrate or even communicate with each other. Managing such an environment costs a lot of time and effort, but what's worse is that the results leave much room for improvement. Hence what Indian manufacturing organizations need to do is try to shift to an integrated security solution that is open, automated and simple to manage.

Perceptions: Security Professionals are Confident about Technology, but are Constrained from Leveraging it to the Fullest

Despite the worsening cyber security climate, Indian organizations are in general very confident about their security arrangements. In the Cisco 2017 Security Capabilities Benchmark Study, 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.

65 percent of respondents from the manufacturing industry also felt the same way. 30 percent of respondents said that while they replaced or upgraded their security technologies at regular intervals, they didn't have the latest tools.

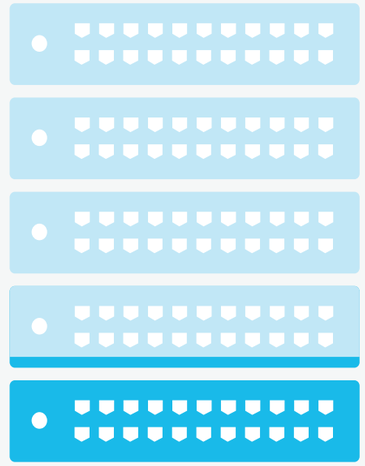
Figure 1. Percentages of Security Professionals in Manufacturing Sector Who Feel Their Security Infrastructure is Up to Date



Described as Very Up to Date

Best Technologies Available

65%



Described as Replaced/Upgraded on Regular Cadence

Not Equipped with Latest and Greatest Tools

30%

2016 (n=23)

Source: Cisco 2017 Security Capabilities Benchmark Study

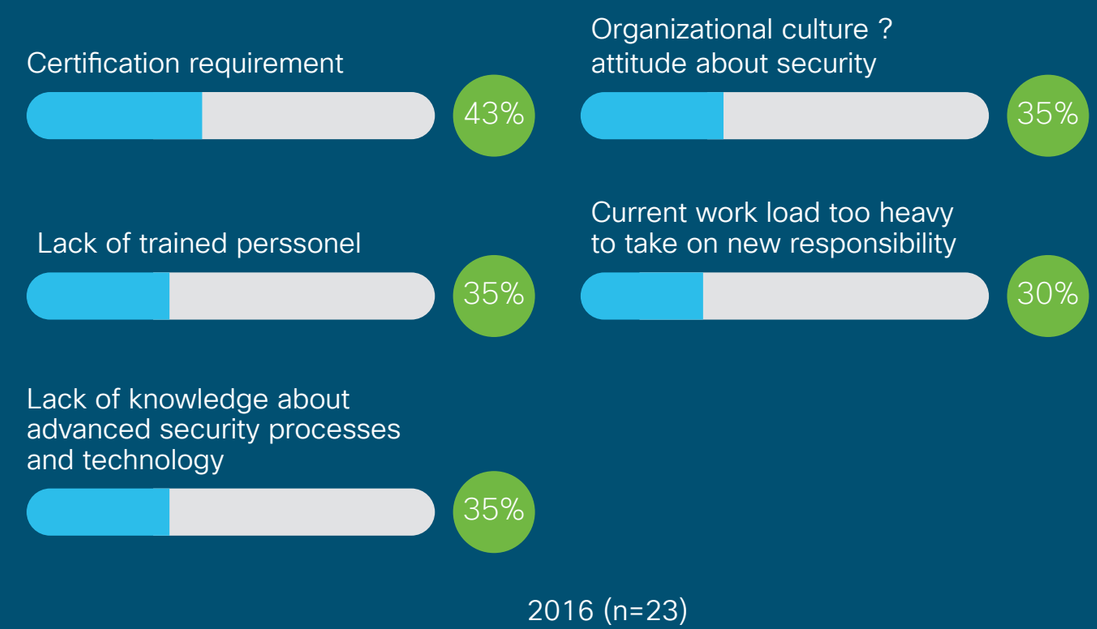
Constraints: Certification Requirements, Absence of Skills and Knowledge, and Cultural Barriers Hamper Manufacturing Organizations from Adopting Security Measures

Indian organizations, which were so confident in their security technology, were less enthusiastic when asked about the implementation of their security solutions and processes. A number of barriers, ranging from the organization's culture and attitude to security, its incompatible legacy systems, and onerous security certification requirements were coming in the way of adoption.

For manufacturing enterprises, the last, namely certification requirements was the biggest issue, called out by 43 percent of respondents, followed by lack of trained personnel, lack of knowledge about advanced security processes and technology, and organizational culture and attitude to security, which were each mentioned by 35 percent of respondents as an obstacle to implementation.

A sizeable 30 percent said their workload was too heavy to allow them to take up new responsibilities such as security. Perhaps they should revisit this opinion given that security is not really an "optional" undertaking for organizations that wish to survive in the digital age.

Figure 2. Biggest Obstacles To Security In Manufacturing Sector



SHARE

Source: Cisco 2017 Security Capabilities Benchmark Study

When an organization uses too many individual security solutions that remain in silos or do not communicate with each other, it can increase its vulnerability to attack. Unfortunately, most security professionals worldwide, and also in India, tend to juggle products from multiple suppliers, which opens up gaps in time and space that hackers can exploit. Overall, 56 percent of Indian organizations use 6 or more vendors, while 69 percent have 6 or more products.

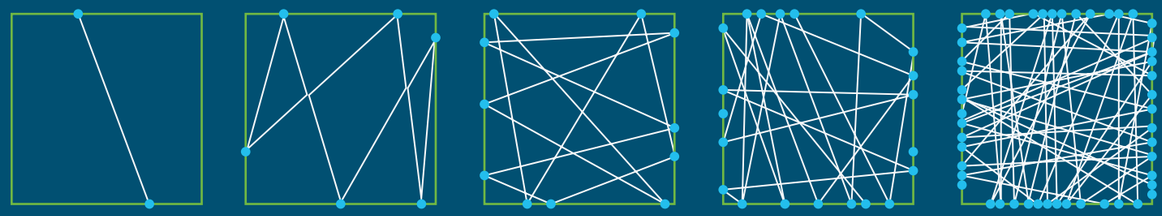
India's manufacturing enterprises also use a lot of security products and vendors. 44 percent of organizations use 6 vendors or more: about a quarter use 6 to 10 vendors, and almost a tenth of companies work with an astounding 21 to 50 vendors.

When it comes to security solutions, 73 percent of companies – nearly three-fourths of the total – use at least 6 products. 43 percent of manufacturers have between 6 and 10 products, 17 percent have between 11 and 25, and 13 percent use between 26 and 50 products.

Figure 3. Number of security vendor And products used by Manufacturing Organizations.

Number of Security Vendors in Security Environment

2016 (n=23), Graphic Rounded to Nearest Whole Number

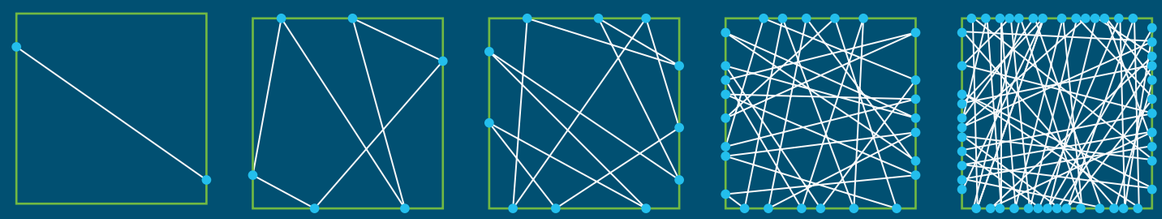


1–5 Vendors	6–10 Vendors	11–20 Vendors	21–50 Vendors	Over 50 Vendors
57%	43%	17%	13%	0%

44% Use More Than 5 Vendors

Number of Security Products in Security Environment

2016 (n=23), Graphic Rounded to Nearest Whole Number



1–5 Products	6–10 Products	11–25 Products	26–50 Products	Over 50 Products
26%	26%	9%	9%	0%

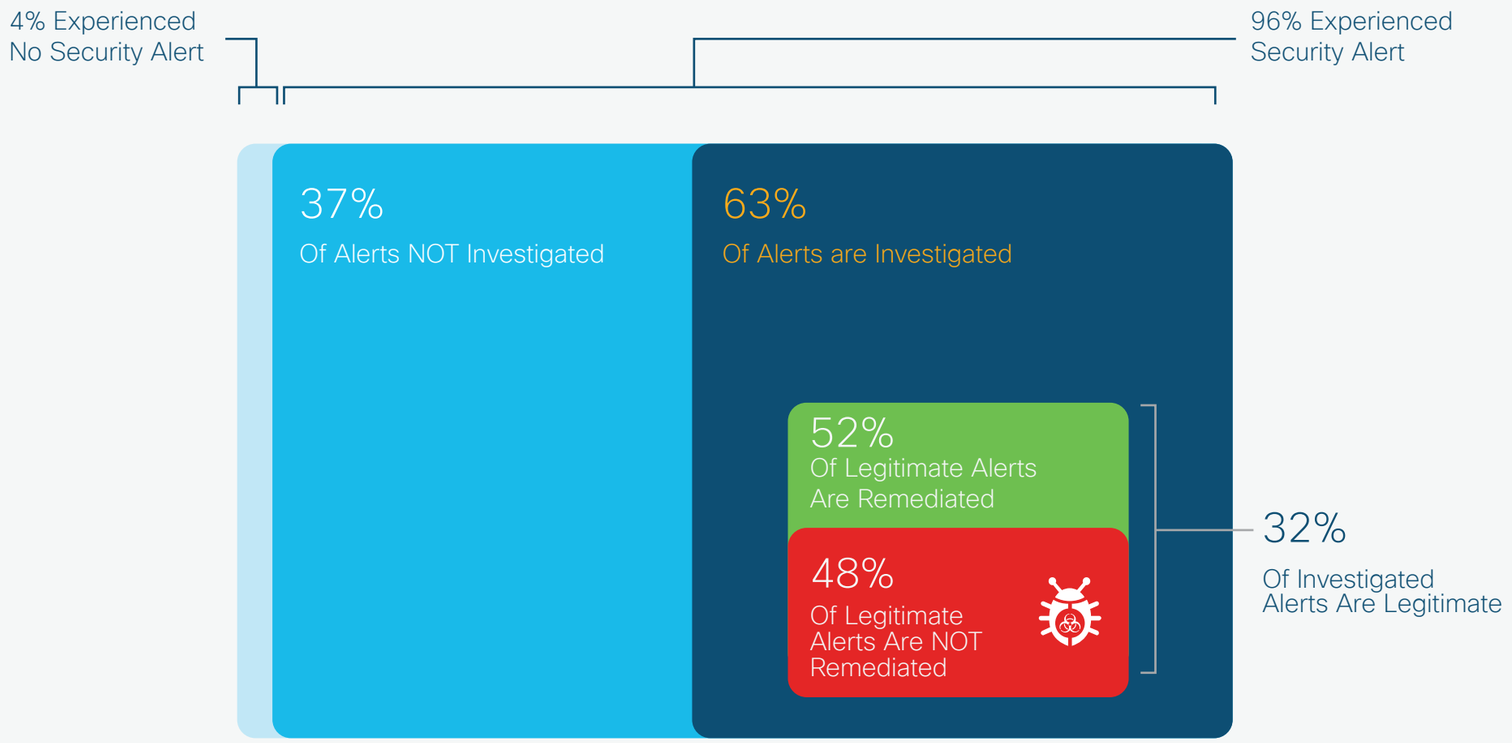
73% Use More Than 5 Products

Source: Cisco 2017 Security Capabilities Benchmark Study

As mentioned in an earlier section, the current security environment in Indian manufacturing organizations is less than optimal. One of the biggest limitations is weak governance. The snarl of security solutions is an obvious factor here, but it is quite likely that the lack of both skilled personnel and knowledge of advanced security processes also contributes to the problem.

Figure 4 shows that manufacturing companies investigate only 63 percent of security alerts, exactly the same as Indian organizations overall. Of these investigated alerts, 32 percent turn out to be legitimate on average. Finally, the companies end up remediating just over half, or 52 percent, of legitimate alerts.

Figure 4. Percentage of security alerts that are Not investigated or remediated by the Manufacturing Sector



2016 (n=23)

Source: Cisco 2017 Security Capabilities Benchmark Study

The following hypothetical example is a stark reminder of the seriousness of the situation.

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

- It investigates 3,150 alerts (63 percent) and ignores 1,850 (37 percent).
- Of the 3,150 alerts that are investigated, about 1,008 (32 percent) are found to be legitimate, while 2,142 (68 percent) are not.
- Of the 1,008 legitimate alerts, the organization remediates only 524 (52 percent) and does not remediate the remaining 484 (48 percent) alerts.

It is worrying that approximately 1 in 3 security alerts go uninvestigated, and 1 out of 2 legitimate alerts are never fixed in the manufacturing industry in India. Organizations must introspect to understand what types of alerts are ignored and why. Do these alerts signal relatively trivial threats that might only spread spam, for instance, or do they pertain to much more serious issues such as a possible ransomware attack or critical damage to a network? Clearly, there is a need to raise the level of investigation. However, given the large number of alerts a typical organization receives every day, it would not be possible for an already burdened security team to investigate them all manually. The solution is to use automation and properly integrated security solutions to probe and analyze a greater area of the threat landscape.

Until then, India's manufacturing companies run the risk of being breached and suffering consequences such as loss of business opportunity, revenue and customers. In the global Cisco Security Capabilities Benchmark Study, a number of respondents said that even small network outages or minor security breaches could make a long-term impact on the company's bottom line. This reinforces the importance of treating even minor incidents with seriousness.

When an organization's defenses are breached, the huge burden of damage control falls on the security team. The study shows that the immediate effects of breach can last quite long. 38 percent of outages in all Indian organizations taken together lasted between 1 and 8 hours; 13 percent lasted 9 to 16 hours; and a similar proportion of outages went on for 17 to 24 hours.

In the case of the manufacturing sector, 55 percent of outages lasted between 1 and 8 hours, 5 percent went on for 9 to 16 hours, and 10 percent lasted for 17 to 24 hours. 16 percent of respondents said that when they had the worst security breach in the past year, it impacted between 1 and 10 percent of their systems. At 32 percent of organizations, the impact was felt on 11 to 30 percent of systems, whereas at 47 percent of organizations, the breach affected 31 to 50 percent of systems.

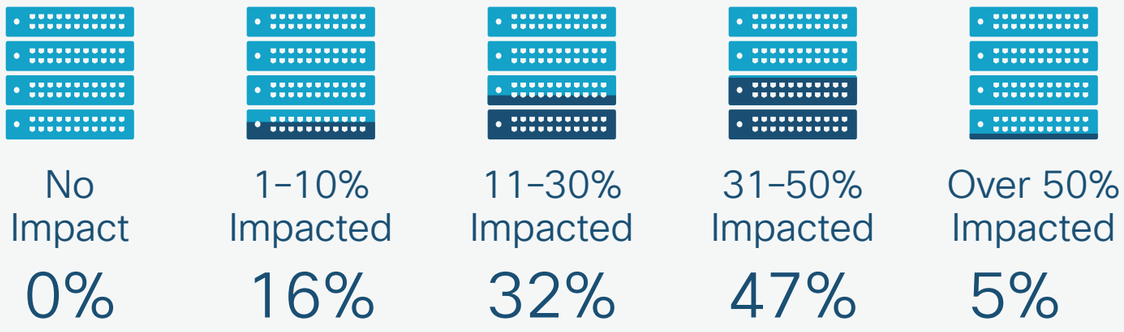
Figure 5. Length and Extent of Outages Caused by Security Breaches in Manufacturing Sector

Organizations' Systems Down Time Due to Breach

2016 (n=20)

Percentage of Systems Impacted Due to Breach

2016 (n=19)



Source: Cisco 2017 Security Capabilities Benchmark Study

Impact: Breaches Cause More than Downtime; Bring Unwanted Publicity, Reduce Performance, Could Damage the Environment and Even Compromise Worker Safety

The effects of breaches aren't limited to outages. Breaches also mean the loss of money, time, and reputation. In the case of manufacturing companies, the implications are far worse, because the breach could cause important equipment to malfunction and put workers' safety at risk.

Security teams who believe they will dodge this bullet are ignoring the reality of the data. As our study shows, a large number of enterprises have had to cope with public scrutiny following a security breach

When their security systems were hacked, 62 percent of organizations in India faced public scrutiny. Manufacturing companies had it even worse, with 70 percent of those suffering a breach coming under the lens of the public. Figure 6 shows that for 38 percent of these organizations, disclosure was involuntary, that is, the breach was made public by a third party. The rest were split down the middle: 31 percent disclosed the breach because they had to by law, while 31 percent did so voluntarily.

The immediate effect of a breach, namely, outage, is usually fixed quite quickly. But other effects can last long into the future. What's more, because the world is such a connected place, news of a breach spreads far and wide and remains in public memory for a while.

If a breach at a manufacturing company impacts the environment or human life, there could be a huge outcry. Hence these organizations should be extra careful about their security infrastructure. Hackers are continually becoming more capable and even more ambitious. Just because an enterprise's systems have not been breached so far does not mean they are impregnable. When it comes to security, one should be too careful.

Figure 6. Percentage of Manufacturing Organizations experiencing a public breach

Source: Cisco 2017 Security Capabilities Benchmark Study

Where are the consequences of a breach likely to be felt by the organization? Worldwide, and also in India, respondents named operations as the function most likely to be affected. The figure for India, at 40 percent, was only slightly higher than the 36 percent reported globally. What this says is that across industries and countries, a security breach poses a real threat to business as usual.

A maximum number of respondents from manufacturing also named operations as the area most likely to be impacted by a breach (57 percent). Next, they named regulatory scrutiny (52 percent), followed by business partner relationships (35 percent) and customer retention (30 percent).

In a highly competitive market, such as India, no organization can afford disruption of key functions. Security professionals in manufacturing enterprises must therefore raise their organizations' defenses against possible attack and also have a plan to get the business back on its feet quickly, should the worst happen.

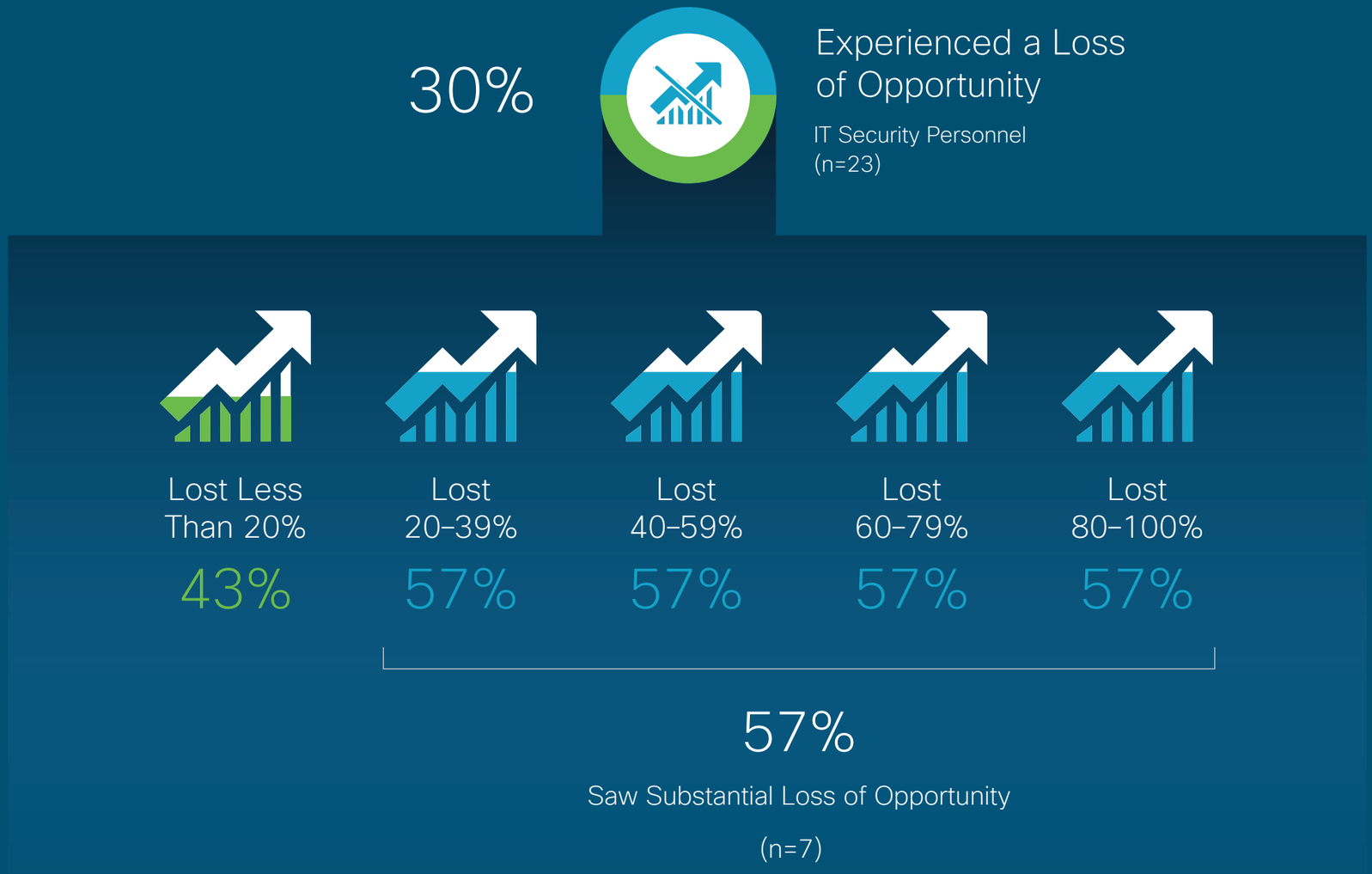
Figure 7. Functions most likely to be affected By a public breach in Manufacturing Sector

Source: Cisco Security Research

Exactly how much have Indian manufacturing companies suffered from a security breach? Figure 8 shows that 30 percent of organizations lost business opportunities, which compares very favorably with the average for Indian organizations overall, at 43 percent.

43 percent of the manufacturing organizations experiencing a loss less than 20 percent of opportunity, and the remaining 57 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).

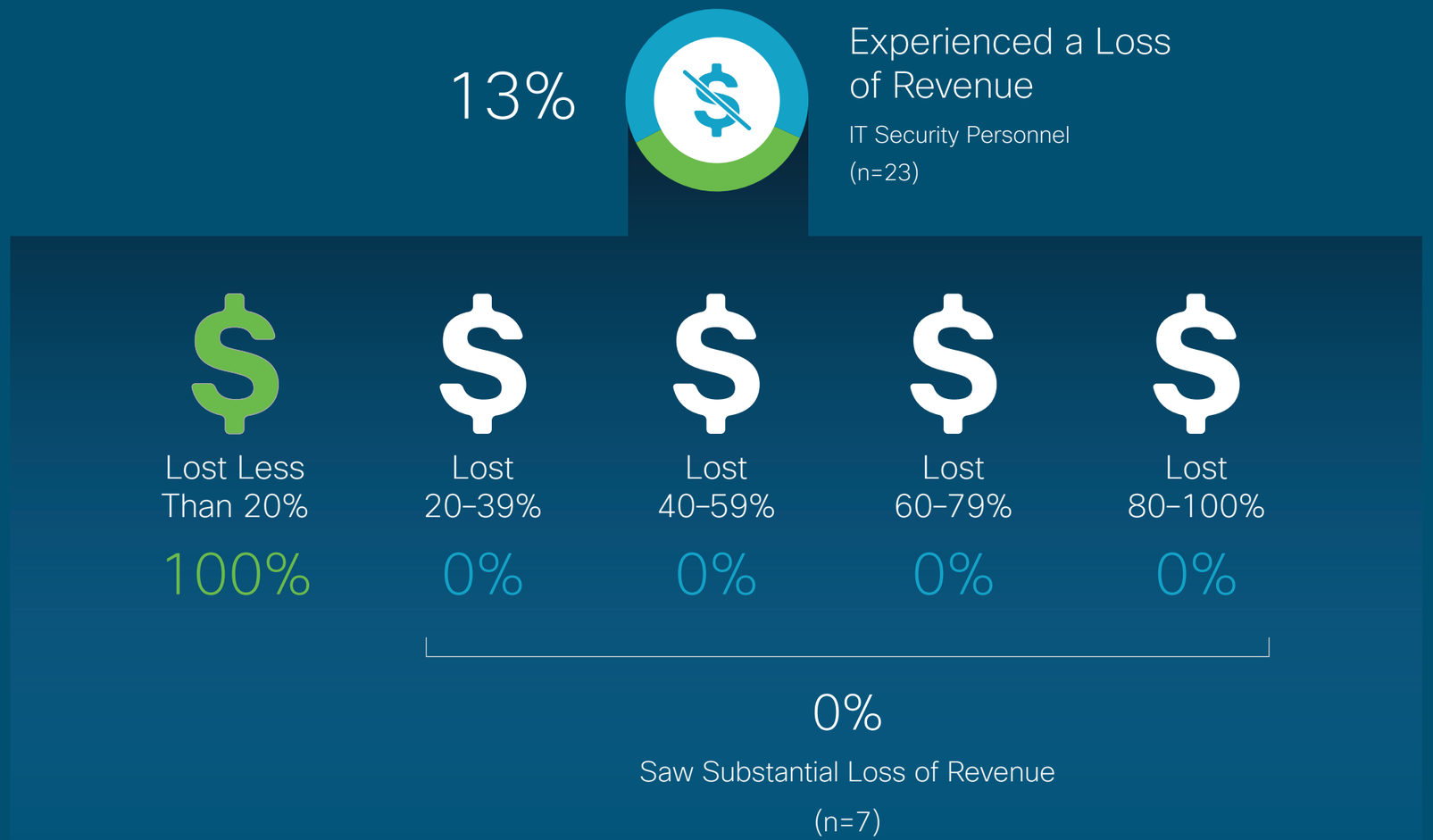
Figure 8. Percentage of business opportunity Lost at the result of attack in Manufacturing Sector



Source: Cisco 2017 Security Capabilities Benchmark Study

A significant proportion of Indian companies, 41 percent to be precise, lost revenue due to attack. Manufacturing companies did much better, with only 13 percent reporting losses. All the losses were small, at much less than 20 percent of revenue.

Figure 9. Percentage of organizational revenue Lost as the result of an attack in Manufacturing Sector



Source: Cisco 2017 Security Capabilities Benchmark Study

Barely any manufacturing organizations (4 percent) in the survey reported losing customers due to a security incident. Once again, the loss was minimal.

Clearly, Indian manufacturing organizations have suffered much less from cyber attack than organizations from other sectors. It would be interesting to probe the reasons for this – is it that these companies have perfected the art of defense, or on the contrary, are they failing to pick the threats? If it is the former, it is indeed good news for the manufacturing industry. That being said, there is no room for complacency and the sector must continue to remain as vigilant as ever, because the threat will only go up in future.

Figure 10. Percentage of customers lost By Manufacturing Organizations due to attacks

Source: Cisco 2017 Security Capabilities Benchmark Study

Outcomes: Greater Scrutiny Means Better Security

A cyber attack can really take a toll on an organization. Unfortunately, even the best-laid defenses are likely to be breached at some point. Hence top management should ensure that their organizations are well prepared to resist, or in the worst case, recover from attack. It is necessary to continually review the company's defenses, and strengthen them by focusing attention and resources on the areas that are most vulnerable.

If a breach occurs despite its best efforts, the company should refrain from despondency or pinning blame, and focus instead on strengthening its security arrangements. The good thing is that Indian organizations do realize this: in the India study, 94 percent of security professionals who had managed public scrutiny due to a security breach said it drove improvements in their organizations.

Manufacturing companies were unanimous that the breaches that resulted in public scrutiny eventually drove them to improve security. 57 percent of security professionals said it increased focus on preventing security breaches caused by employee-owned mobile devices. At 50 percent of companies, the improvement resulted in better enforcement of data protection laws and regulations, greater focus on risk analysis and mitigation, higher investments in security defense technologies or solutions, and more security awareness training for employees.

From these responses, it appears that employees are one of the biggest sources of vulnerability in manufacturing organizations, quite likely because they use their personal devices at work. This puts the organizations in a quandary – how much can they restrict the use of personal devices at work, or accessing of Internet sites from official computers, without curtailing employee productivity and freedom?

Figure 11. How security breaches drive Improvements in Manufacturing Sector

100% Said Security Breach Drove Improvements in Threat Defense Technologies, Policies, or Procedures

Security Professionals (n=14)

Top 5 improvements made to protect company from security breaches

2016 (n=14)

57% Increased focus on preventing security breaches caused by employee owned mobile devices

50% Increased enforcement of data protection laws and regulations

50% Increased focus on risk analysis and risk mitigation

50% Increased investment in security defence technologies or solutions

50% Increased security awareness training among employees

Source: Cisco Security Research

As mentioned earlier, a solid majority of organizations in India, and in manufacturing, faced public scrutiny after suffering a cyber attack. Scrutiny can come from a variety of stakeholders, who are also usually impacted by the incident.

91 percent of manufacturing companies in India expected scrutiny from clients and customers, while 87 percent thought it would come from regulators, executive leadership and employees. Relatively fewer respondents (61 percent) believed they would be questioned by the press.

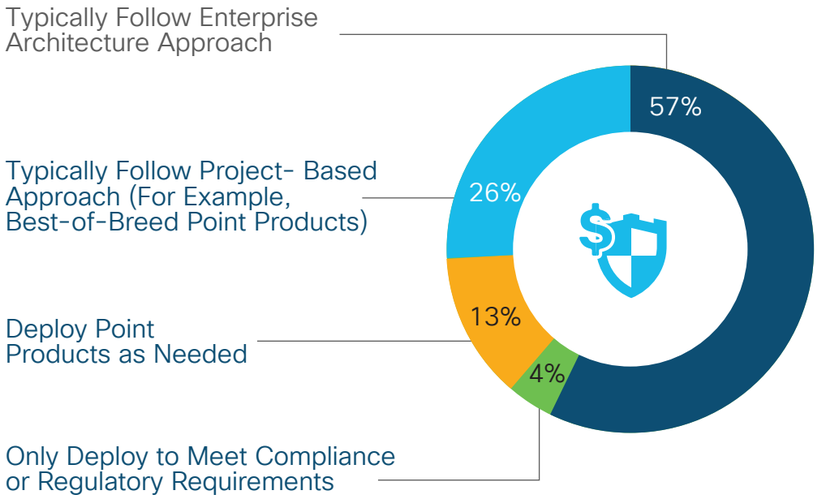
Figure 12. Sources of Increased Security in Manufacturing Sector

Source: Cisco 2017 Security Capabilities Benchmark Study

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

Security Threat Defense Solution Purchasing

IT Security Personnel (n=51)

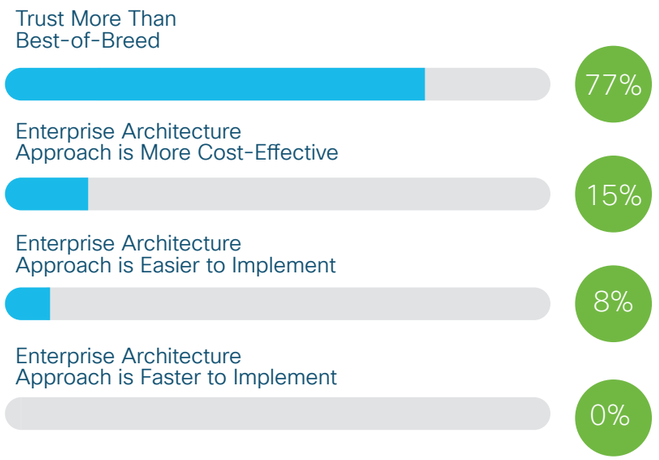


Reasons for Favoring a Best-of-Breed Approach

Organization That Purchased Best-of-Breed Point Solutions

Reasons for Favoring an Enterprise Architecture Approach

Organizations That Typically Follow an Enterprise Architecture Approach



Trust Versus Cost: What Drives Security Purchases?

The goal of all security professionals is to ensure the best defenses for their organizations, although their paths may differ. The two most commonly used options are to buy best of breed point solutions from different vendors or use an integrated enterprise architecture approach. The Indian manufacturing industry differs from other sectors in that it prefers an integrated architecture approach (named by 57 percent) to buying a number of best of breed point solutions (26 percent).

There are different motivations behind these choices. For the security professionals in Indian manufacturing companies who do favor the best of breed approach, the key factor is speed of implementation (cited by 50 percent). On the other hand, trust clearly drives the decision to go for an enterprise architecture solution (77 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. Point solutions save time and cost during implementation, but 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, and uses automation to detect threats faster.

Summary: What the Benchmark Study Reveals

If the presence of the latest security tools and technologies automatically meant foolproof security, the world would be a safer place. Unfortunately, the study shows that it is anything but the case. The way organizations put their solutions to work, their security policies and procedures, and the level of governance are as important in safeguarding their boundaries. Currently, manufacturing companies face several constraints, including difficulty in obtaining certification, lack of skilled security personnel, inadequate knowledge about advanced security processes and technology, and cultural barriers that prevent them from leveraging their security infrastructure to the fullest. And while the manufacturing industry is ahead of other sectors in switching to an integrated architecture approach to security, it still uses a number of point solutions that drag it down.

These obstacles must be dismantled at the earliest to clear the path to adoption.
But even after that, there is a risk that systems will be breached someday. The survey shows that manufacturing enterprises have lost much less business opportunity, revenue and customers than the average Indian organization. Even so, they should never let their guard down, and must help their security teams to work around their constraints as far as possible.
Here, the commitment and leadership of top management is the key to building a supportive culture and attitude towards cyber security throughout the organization.

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