

REPORT

Third-Party Cyber Risks to Global Supply Chains

A Security Assessment of Key Indian Suppliers



Introduction

India's rapidly expanding economy has cemented its position as a critical hub in global supply chains across multiple high-impact industries, from semiconductors and aerospace to IT services and life-saving pharmaceuticals. This interconnection delivers efficiency and cost advantages, but it also amplifies cyber exposure.

SecurityScorecard's latest research reveals that the security weaknesses present in Indian suppliers are both more widespread and more severe than our analysts initially anticipated, creating significant potential for cascading third-party breaches that can affect organizations worldwide.

Our analysis found that 52.6% of Indian companies in the sample experienced at least one third-party breach. This is a rate of exposure that should concern any organization relying on India for manufacturing, technology services, or specialized components. The threat does not stop at direct connections. Indian companies themselves rely on a web of suppliers, creating fourth-party risks that extend even further into the global supply chain. A single ransomware incident or disruptive cyberattack affecting one Indian vendor could halt production lines, delay service delivery, or disrupt critical logistics for companies in multiple countries.

Security ratings for key Indian suppliers revealed a sharply divided picture. At one end of the spectrum are strong performers with robust defenses. At the other are companies with dangerously weak security postures. Even when adjusted for the lower average ratings often seen in developing economies, the average scores in the Indian sample remain low.

The extremes are especially notable when broken down by sector.

- Indian firms in information technology and aerospace recorded the highest average scores, significantly outperforming their peers
- While semiconductor manufacturing, other electronics, pharmaceuticals and medical devices, automotive, and textiles recorded some of the lowest.

These low-scoring manufacturing sectors are strategically important to the global economy and are consistently

targeted by cybercriminals. Supporting data shows higher-than-average levels of typosquatting, compromised credentials, and device infections in these industries, all of which can be exploited to achieve initial compromise.

IT Sector

The IT sector deserves special attention in the Indian context. Globally, IT providers face elevated cyber risk because of their central role in enabling third-party access, their large and complex attack surfaces, and their attractiveness as high-value targets.

- In India, despite significantly higher-than-average security scores, IT companies in our sample still recorded large volumes of typosquatting domains, credential compromises, and infected devices.
- They also experienced some of the highest rates of publicly reported breaches, particularly third-party breaches that can allow attackers to bypass the more robust defenses of their primary targets.
- In fact, half of all publicly reported third-party breaches in our study involved Indian IT firms.

The high level of risk tied to outsourced IT operations and managed service providers was especially striking, with these services responsible for 62.5% of all third-party breaches in our sample. This is the highest proportion our researchers have ever documented and raises urgent questions about the resilience of global businesses that rely heavily on Indian IT vendors.

Pharmaceutical Sector

Pharmaceuticals and medical devices represent another industry of concern. While their security scores were already below average, their real vulnerability was reflected in breach outcomes. This sector accounted for 42.1% of publicly reported breaches and 38.5% of ransomware attacks among the Indian companies we studied.

Disruptions in this industry can have profound consequences for global healthcare supply chains. During the height of the COVID-19 pandemic, for example, a cyberattack on an Indian pharmaceutical firm delayed clinical trials for a vaccine, demonstrating how a local incident can produce worldwide effects.

Key Red Flags

When examining the root causes of weak security ratings among Indian companies, we found that network security factors—especially those related to certificate management—were the most common contributors. This finding diverges from patterns we have seen in both U.S. and global datasets, where other factors tend to dominate.

The diversity and number of network security issues were higher than usual, and unsatisfactory patching cadence was also unusually common. This slow approach to patching often correlates with broader weaknesses in security posture, and our analysis confirms that underperformance in patching cadence is linked to higher overall cyber risk.

Implications

The implications for technology and security leaders are clear. For CISOs and IT directors managing complex ecosystems of suppliers and service providers, the cyber health of Indian partners is not a peripheral concern. It is a central factor in business continuity and operational resilience.

For the broader technology community, these findings underline a critical truth: in an interconnected global economy, your security is only as strong as the most vulnerable partner in your supply chain.

Key Findings

- **Average security scores for our sample are extremely low, with a mean of 73 and a median of 75.** The largest concentration of scores (26.7%) is in the “F” letter grade range, and many of those “F” scores are extremely low, even for that already low range.
- **Nonetheless, the sample’s second-largest share of companies (25.3%) has scores in the highest “A” letter grade range.** This unusual distribution suggests a heavily polarized sample, with the largest concentrations of companies at either end of the scale.
- **Security scores vary massively by industry.** Two industries had far higher average scores: IT (91/95) and Aerospace & Aviation (82/89). The high IT scores are surprising for an industry that usually underperforms (compared to its peers) in other regions..
- **Five industries, all of which involve manufacturing, have average scores even lower than those of the whole sample:** Semiconductors (70/71), Other Electronics (68/73), Pharmaceuticals & Medical Devices (66/72), Automotive (67/69), and Textiles (67/68). This trend is a more pronounced version of the common tendency of manufacturing organizations to score lower than their peers in most other samples.
- **This sample is unusual in that: a) Network Security is the risk factor for which the largest share of companies (31.3%) have the lowest sub-scores; and b) those lowest sub-scores were lower than usual, compared to the most common lows elsewhere.** In other words, Network Security is not only more common as the greatest risk factor in India, it has a worse impact on security than the most common risk factors elsewhere.
- **Individual Network Security issues were also the most common sources of the most negative score impact in this sample (46.7%).** This sample also contained a greater number and wider range of individual Network Security issues than most other samples. Many of these issues involved expired or revoked certificates.
- **Patching Cadence was significantly more common (at 20%) as the security risk factor with the lowest sub-scores.** Prior research indicates that companies scoring lowest in Patching Cadence tend to score lower in general, highlighting this risk factor as a red flag for more widespread problems in other areas. The unusual salience of Patching Cadence risk in this sample thus fits the sample’s unusually low ratings in general.

- **Four industries are top targets of typosquatting domains: IT, Semiconductors, Other Electronics, and Automotive.** IT is a popular, high-value target for threat actors and thus likely to have more typosquatting domains, despite the high security scores for that industry in our sample. The other three industries are both strategically significant targets and involve manufacturing. Manufacturing organizations often have weaker security programs in general, making them less likely to takedown typosquatting domains.
- **IT and Other Electronics companies were overrepresented among companies with the most compromised credentials.** IT companies are not only popular targets, but their larger, more complex attack surfaces give attackers more accounts to compromise, even if their security scores are higher. Nonetheless, the high-scoring Aerospace & Aviation industry was overrepresented among the companies with zero compromised credentials.
- **12% of the sample (18 companies) has at least one compromised device on their networks.** All but one of those companies had an adware infection. A large minority (41.2%) of adware-infected companies also had either a maliciously repurposed device or an infection with a type of malware other than ransomware or an information stealer.
- **The distribution of device compromises indicates a clear emphasis on three industries: IT, Semiconductors, and Other Electronics.** The “most infected” company was a Semiconductors company with a low “F” grade and more than twice as many compromised devices as the next-most compromised company.
- **10.7% of the sample (16 companies) have had publicly reported breaches.** Three companies had two publicly reported breaches each, yielding a total of 19 breaches. These proportions are surprisingly low, suggesting a possible underreporting problem.
- **Almost three-quarters (73.7%) of the publicly reported breaches are in just two industries: IT and Pharmaceuticals & Medical Devices.** IT companies are high-value targets and are more often on both ends of third-party cyber risk, making them more susceptible to breaches despite their high security scores in India. The numerous attacks on Pharmaceuticals & Medical Devices likely reflect issues separate from the widespread targeting of the broader Healthcare industry in the U.S. and other advanced economies.
- **Our sample had a relatively high rate (52.6%) of third-party breaches.** Exactly half (50%) of them affected the IT industry, which helps to explain why that industry had such a high proportion of breaches in general, despite its higher security scores.
- **Third-party IT products & services enabled 80% of the third-party breaches in our sample - the highest percentage we have documented thus far.** The most common third-party attack vector of this kind (62.5%) was the use of outsourced IT operations or managed service providers (MSPs).
- **68.4% of the breaches in our sample involved ransomware.** We also observed a close correlation between ransomware and third-party breaches, consistent with other U.S. and global samples. 38.5% of these ransomware attacks were also third-party breaches, and 60% of the third-party breaches also involved ransomware.
- **38.5% of ransomware attacks in our sample affected Pharmaceuticals & Medical Devices.** Unlike the more general attacks on this industry, the reasoning behind these ransomware attacks on this industry was more consistent with the well-known popularity of ransomware attacks on the broader Healthcare industry in the U.S. and globally.

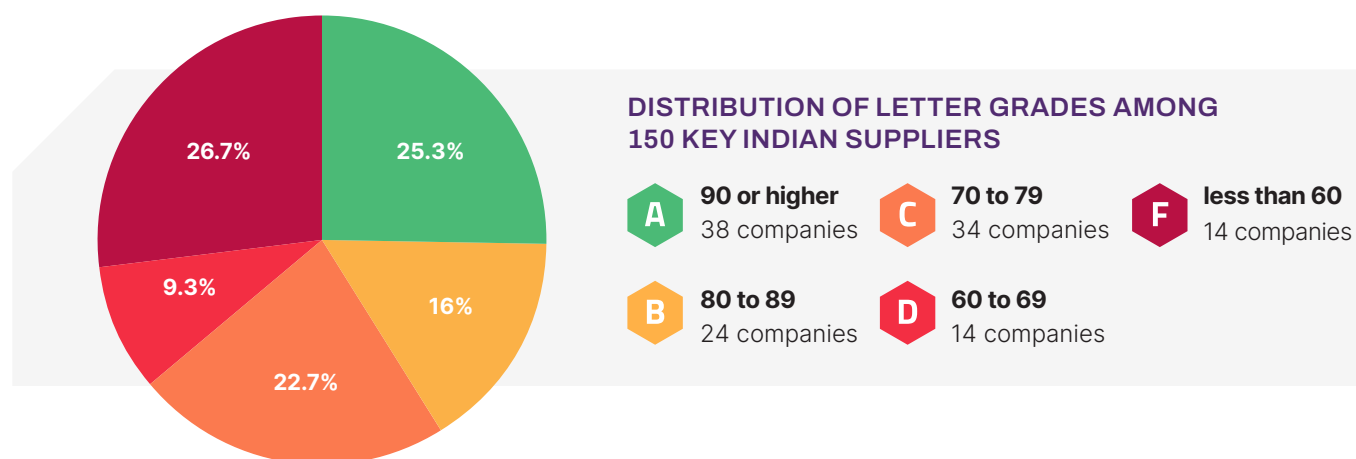


General Statistics

The mean score for these 150 companies is 73; the median score is 75. As with most of our other industry-specific samples, the lower mean score indicates that the sample is somewhat “left-skewed,” i.e. a few extremely low scores at the lower end of the range drag down the value of the mean. The median value may thus be a better representative of the whole sample.

In any event, 73/75 are relatively low mean/median scores. For comparative context, the mean score for the 12 million organizations around the world and across all industries that our platform covers is 81. 73/75 are also the lowest mean/median scores, by a wide margin, that we have encountered in any sample of private sector organizations that we have analyzed in the past 18 months.

For example, our lowest-scoring private sector sample to date, the world’s [150 top technology vendors](#), had much higher mean/median scores of 84/87. Most of our other samples of major U.S. and global businesses typically have mean/median scores in the mid-high 80s.



According to our scoring methodology:

- A “B” rating indicates a 2.9x greater likelihood of a breach than an “A.”
- A “C” indicates a 5.4x greater likelihood than an “A.”
- A “D” indicates a 9.2x greater likelihood than an “A.”
- An “F” indicates a 13.8x greater likelihood than an “A.”

“A” is strong/excellent, “B” is good/decent; and “C,” “D,” and “F” are mediocre/deficient/bad.

This distribution of letter grades is unusual and unfavorable. The largest share of the sample, representing more than a quarter of it (26.7%), consists of companies with “F” grades of 60 or less. Even this figure fails to capture the extremely low scores of some companies, which range from 32 to 59. Three of them (2% of the whole sample) are in the 30s, 22 of them (14.7% of the sample) are in the 40s, and 15 of them (10% of the sample) are in the 50s.

Our researchers have not previously encountered a sample in which companies with “F” grades constituted the largest share, **nor have we seen so many low scores that fall so far into the “F” range.**



Nonetheless, the second-largest share of the sample, by a margin of just two companies (1.4%), consists of those with “A” grades of 90 or higher (38 companies, or 25.3%).

This distribution is thus even more unusual in its polarization; the two largest shares of the sample are at the most extreme ends of the scale. While this large share of companies with scores in the highest possible range does somewhat balance out those with low scores, it is nonetheless a relatively small share compared to those of most other U.S. and global samples. Companies scoring in that highest “A” range typically constitute 30-40% or more of total U.S. and global samples.

As if to balance out this polarization of scores at both extreme ends of the scale, the third-largest proportion of scores (34 companies or 22.7%) falls within the middle “C” range of mediocre scores just above failure. In other words, nearly three-quarters (74.7%) of the whole sample falls into one of these three top categories at the highest, middle, and lowest points on the scale: “A” for excellent; “C” for mediocre; and “F” for failure.

The remaining quarter or so (38 companies or 25.3%) fall into either the unusually small “B” range (24 companies or 16%) or the unusually large “D” range (14 companies or 9.3%). We have not seen this unusual distribution in prior samples, most of which resemble an “inverted pyramid,” with most scores concentrated at the higher end of the scale and fewer and fewer scores as one moves down the scale.

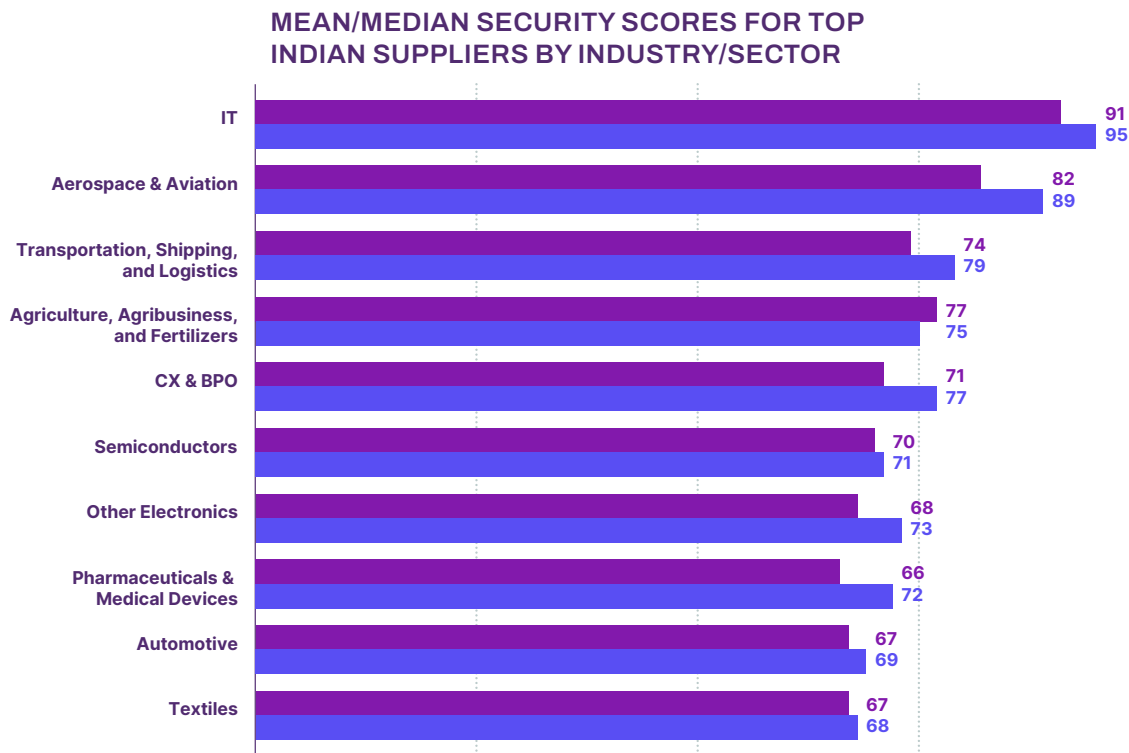
While the wide margin by which this Indian sample underperformed by international standards came as a surprise to our analysts, the mere fact of the lower scores was not. [Our previous research established a strong correlation between GDP per capita on one hand and security scores on the other.](#) Generally speaking, businesses in more affluent and advanced economies tend to have higher security scores and vice versa.

Businesses in more affluent economies tend to have more money to spend on more robust security programs, and vice versa. While India has a large economy with many advanced segments (some of which are likely reflected at the higher end of this polarized sample), it still remains a developing country with widespread poverty. Nonetheless, the degree to which these Indian businesses underperformed as a whole was greater than one would expect when one accounts for this economic variable.

Relatively low costs are one reason that India has become a popular source of suppliers for global businesses based in more advanced and affluent economies. The same low operating costs that make India an attractive source of suppliers may also account for much of the poor security hygiene that these low scores reflect. In other words, “you get what you pay for.”

Variations by Industry

We further analyzed these 150 mean/median scores by industry in search of variations.



Two industries stand out with mean/median scores well above-average for the sample: IT and Aerospace & Aviation. The massive gap between the high IT scores and the average for the sample came as a surprise. In most other U.S. and global samples, IT companies tend to score below-average relative to their peers in other industries. Their larger and more complex attack surfaces often give attackers more opportunities to find gaps that defenders may have missed. Their utility as third-party attack vectors against their customers makes them popular targets. Indeed, even in purely absolute terms, the A-range IT scores for this sample were higher than what we typically find at IT companies in the U.S. and other advanced and affluent economies.

The significantly above-average scores for Aerospace & Aviation are somewhat less of a surprise, [despite our previous analysis of that industry](#), which found it to be in the middle of the pack in terms of scores. The greater sensitivity and safety implications of that industry's products & services and its connections to military and national defense establishments could account for the creation of a more security-conscious business culture than in other industries.

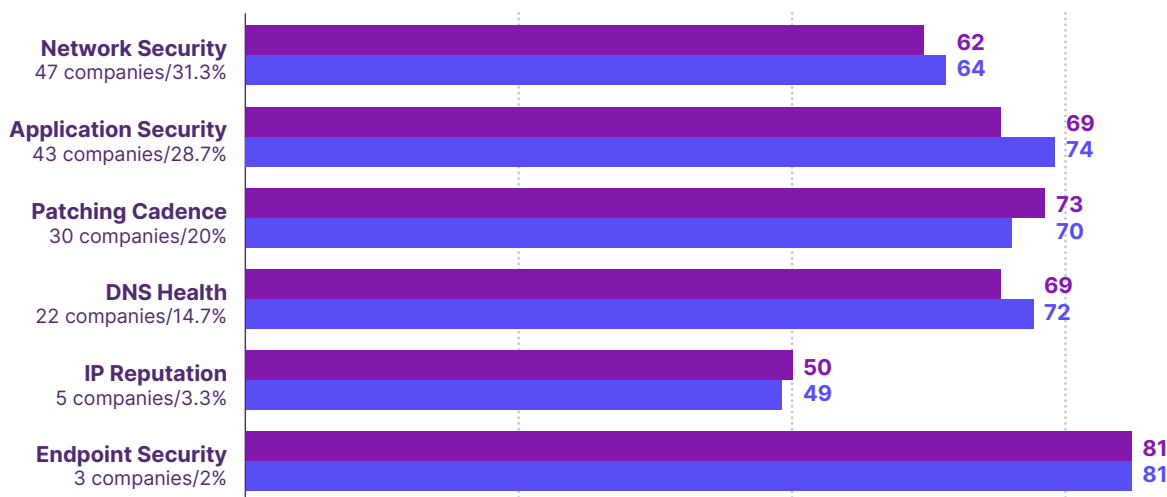
Slightly above average, by a far smaller margin than the other two industries, is another surprise: Agriculture, Agribusiness, and Fertilizers. Our analysts cannot explain why this sector would score above-average for the sample, except to note that some agricultural fertilizers may involve valuable intellectual property (IP) that their developers would want to protect. CX & BPO (which includes the well-known Indian call center industry) almost matches the national average.

Five other industries score below-average relative to the whole sample. All five involve some manufacturing, whose businesses tend to score lower than their peers in most other U.S. and global samples, albeit not by such wide margins. Four of those industries have strategic economic importance or sensitivity: Semiconductors, Other Electronics, Pharmaceuticals and Medical & Technology & Devices; and Automotive. The low scores for Semiconductors and Other Electronics are troubling in light of U.S. efforts to shift from dependence on Chinese manufacturing and towards Indian alternatives. The low Pharmaceuticals & Medical Devices scores raise concerns about the protections of the high-value IP that these companies handle and the often life-saving functionality of the medical devices that they produce. Automotive supply chains are vulnerable to disruptions of their manufacturing operations.

The Most Common Security Risk Factors

For each company in our sample, we identified the one of 10 security factors for which it received its lowest sub-score, which are components of its overall score. Below are the numbers and percentages of companies scoring lowest in each factor, along with mean/median sub-scores for those companies that scored lowest in those security factors. Note that only six of the 10 security factors by which we rate an organization's security appeared on this list at all.

PERCENTAGE OF COMPANIES SCORING LOWEST IN EACH SECURITY FACTOR, WITH THEIR MEAN/MEDIAN SCORES FOR THOSE FACTORS



This distribution of lowest-scoring security factors is unusual in several ways. This sample is the first one in which we have identified a security factor other than Application Security as the most common source of the lowest sub-scores. Application Security dominates most samples with shares in the 30-40% range or even higher, occasionally accounting for a majority of lowest scores. It was less surprising to see Network Security displace Application Security as the most common source of the lowest sub-scores.

This security factor often comes in second or third place in other samples, and it includes one of the most common security issues to have the most negative impact on security scores (which we will discuss further below).

Almost equally unusual are the relatively low mean/median sub-scores for those companies scoring lowest in Network Security. Normally, the mean/median sub-scores for the most common source of lowest sub-scores (which has always been Application Security until now) are usually among the highest. This trend suggests (somewhat counterintuitively) that security flaws in that area may be among the most common but may also have relatively mild or moderate impacts on overall scores, which are usually higher than in this sample.

In contrast, in the case of this unusually low-scoring Indian sample, the most common source of the lowest sub-scores (Network Security) also has some of the most severely negative impacts on overall scores, in a more intuitive relationship than in most other samples. In other words, Network Security is both a more common and a more severe problem area for our Indian sample than it is internationally,

Another unusual feature of this sample is the salience of Patching Cadence as the third-most common source of the lowest sub-scores, accounting for exactly one-fifth of them (20%). Patching Cadence is usually close to the bottom of these lists and typically accounts for a much smaller percentage of lowest sub-scores, typically in the single digits.

Furthermore, we have previously identified Patching Cadence, along with IP Reputation, as “canary in the coal mine” security factors.

Companies that score lowest in these two areas often have lower overall scores in general, suggesting that poor performance in one or both of these areas is a red flag hinting at deeper and more widespread problems in other areas.

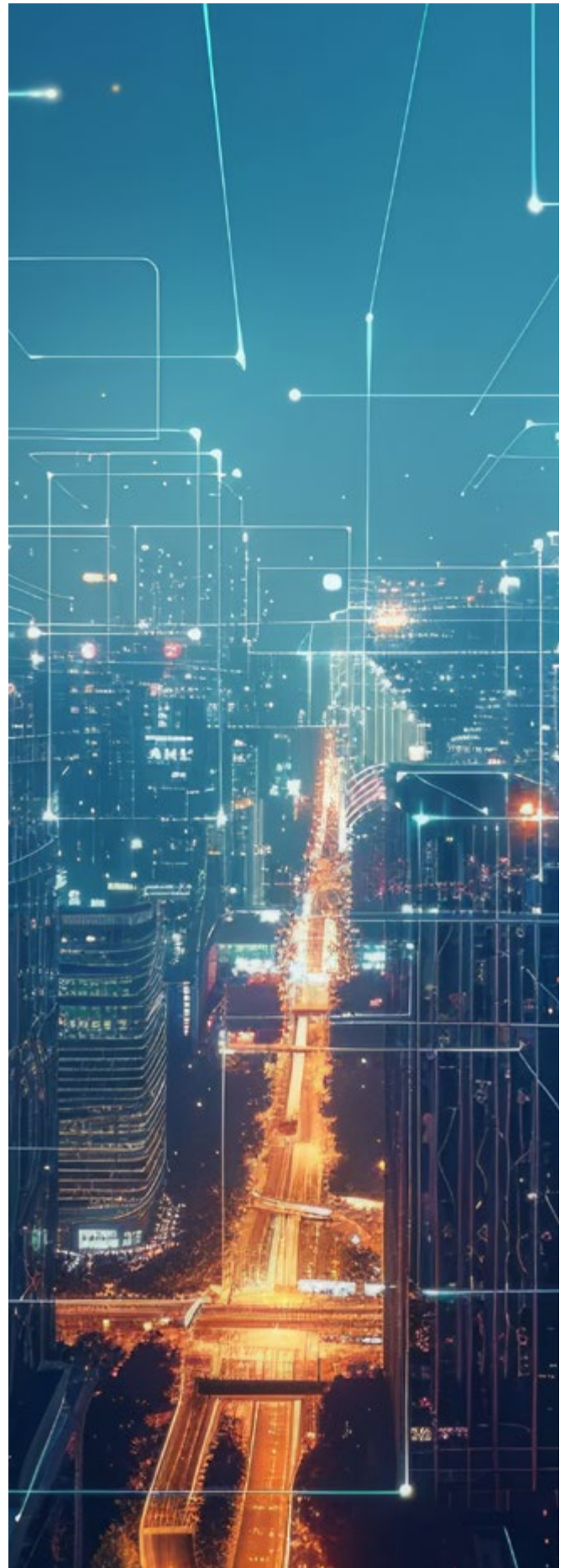
It is thus not surprising that Patching Cadence is such a common source of lowest-subscores in a sample that scored so low in general. In other words, the unusual prominence of Patching Cadence as a security problem for companies in this sample reflects a sub-par security posture, on average and in general.

In contrast, IP Reputation scores in this sample were consistent with those of other samples.

Relatively few companies scored lowest in this security risk factor, but those few that did suffered heavily from it, with the lowest mean/median subscores coming from this factor (50/49).

One bright spot on this list is Endpoint Security. Not only was it the least common source of the lowest-subscores (just 2% of them), those companies scoring lowest in it also had the highest sub-scores for this lowest-scoring risk factor of theirs (81/81).

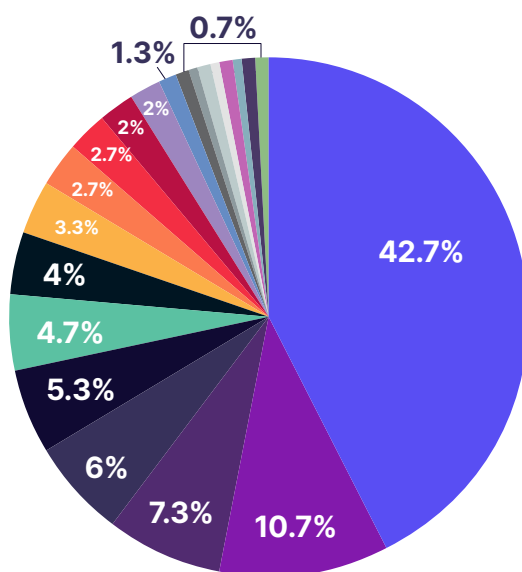
In other words, the security posture of those few companies weakest in Endpoint Security suffered relatively little from it.



Specific Security Issues

We delved further into the individual security issues on which these subscores for each security factor are based. We identified the specific issues that had the most negative impact on the scores of each company. Below are the relevant percentages for each individual issue. The security factor under which each issue counts is in parentheses.

SECURITY ISSUES WITH MOST NEGATIVE SCORE IMPACT FOR EACH COMPANY



- SSL/TLS Service Supports Weak Protocol (Network Security): 64 companies/42.7%
- Session Cookie Missing "Secure" Attribute (Application Security): 16 companies/10.7%
- Unsafe Implementation of Subresource Integrity (Application Security): 11 companies/7.3%
- Session Cookie Missing "HTTPOnly" Attribute (Application Security): 9 companies/6%
- SPF Record Contains a Softfail without DMARC (DNS Health): 8 companies/5.3%
- Outdated Web Browser Observed (Endpoint Security): 7 companies/4.7%
- Redirect Chain Contains HTTP (Application Security): 6 companies/4%
- SPF Record Missing (DNS Health): 5 companies/3.3%
- Certificate is Expired (Network Security): 4 companies/2.7%
- High-Severity Vulnerability in Last Observation (Patching Cadence): 4 companies/2.7%
- Medium-Severity Vulnerability Patching Cadence (Patching Cadence): 3 companies/2%
- Site Does Not Enforce HTTPS (Application Security): 3 companies/2%
- Website References Object Storage (Application Security): 2 companies/1.3%
- Certificate is Revoked (Network Security): 1 company/0.7%
- DNS Server Accessible (Network Security): 1 company/0.7%
- LDAP Server Accessible (Network Security): 1 company/0.7%
- Telnet Service Observed (Network Security): 1 company/0.7%
- Potentially Vulnerable Application Installation (IP Reputation): 1 company/0.7%
- Low-Severity Vulnerability in Last Observation (Patching Cadence): 1 company/0.7%
- Critical-Severity Vulnerability Patching Cadence (Patching Cadence): 1 company/0.7%
- SSH Supports Weak Cipher (Network Security): 1 company/0.7%

Network Security issues in the aggregate accounted for almost half of the list (70 out of 150, or 46.7%). Most of those Network Security issues fell under the rubric of weaknesses in SSL/TLS protocols, such as weak cryptographic algorithms, outdated libraries, or misconfigured settings, with that one issue alone accounting for 42.7% of the whole list. This issue dominates our other U.S. and international samples by similarly wide margins, so it was not a surprise to see it at the top of this Indian sample's list either. More unusual is that there were several other Network Security issues that made it onto the list, thus contributing to the unique position of Network Security as the risk factor most likely to have the lowest subscores in our India sample. These other Network Security issues included certificates that were either expired (4) or revoked (1).

Application Security issues in the aggregate accounted for almost one-third of the list (47 out of 150, or 31.3%) - somewhat higher than the 28.7% for this overall risk factor noted above. The high number and this higher percentage of aggregate Application Security issues is more consistent with what we have seen in other U.S. and international samples. Many of these Application Security issues also involve weak or absent encryption practices, such as:

- The absence of cookie attributes ensuring that they travel via encrypted HTTPS to prevent interception, and not via insecure alternatives that attackers can use
- A lack of subresource integrity (SRI) checks on the cryptographic hashes of external resources loaded to websites, so as to prevent attackers from injecting malicious scripts
- The use of unencrypted HTTP in redirect chains, exposing data to interception and manipulation and increasing the risk of man-in-the-middle (MITM) attacks and phishing

More unusual is the salience of multiple Patching Cadence issues, ranging in severity from low to critical. It is unusual for these issues to make it onto these lists in other samples. As we established earlier above, Patching Cadence in general is a far more widespread and severe risk factor for this Indian sample than it has been for most of our U.S. and international samples. It is thus not surprising that so many Patching Cadence issues would make it into this list.



Typosquatting Domains

Our platform tracks domains suspected of “typosquatting” or spoofing the real domains of organizations that our platform covers. Such malicious domains aim to lure users seeking the real websites with similar but not identical domain names with common typos, misspellings, or subtly inaccurate spoofs of real domains’ character strings. Such domains can serve malicious purposes, such as phishing or camouflaging malware command-and-control (C2) infrastructure.

Organizations should monitor the creation of potentially malicious domains spoofing their own legitimate ones and request takedowns. Variations in the numbers of typosquatting domains can shed light on variations in companies’ security postures and threat actors’ targeting priorities.

The numbers of typosquatting domains for the 150 companies in our sample ranged from 0 to 859. 68 of the 150 companies (45.3%), had no typosquatting domains at all. The mean number of typosquatting domains was 54; the median number was 4.

If one excludes the 68 companies with no typosquatting domains, the mean number of typosquatting domains among the 82 remaining companies with at least one typosquatting domain is 99; the median is 55.

The much greater mean values, compared to the median values, indicates that this data set is “right-skewed.” In other words, the larger values at the higher end of the scale are inflating the mean values, whereas the median values may be a more accurate representation of the data set.

An analysis of the distribution of typosquatting domains yielded some industry-specific insights.. For example, among the 68 companies with no typosquatting domains, some industries were underrepresented, whereas others were overrepresented.

For example, only one company out of 15 from the heavily targeted IT industry made it onto this list. The high security scores of IT companies in our sample may reflect stronger security cultures, but whatever efforts they make to take down typosquatting domains may not be enough to outweigh their high value as targets.

In contrast, 11 of the 15 companies from the Agriculture, Agribusiness, and Fertilizers industry, which had above-average scores and may be lower-priority targets, made it on this list.

Further analysis of the 40 companies with a number of typosquatting domains equal to or greater than the above median of 55 yielded more insights. Four industries were overrepresented: IT, Semiconductors, Other Electronics, and Automotive.

We already established that IT companies are high-priority targets, perhaps enough to outweigh their higher security scores. The other three industries had below-average security scores in our sample, and their businesses involve manufacturing, a field in which companies tend to score lower in general, regardless of what or where they manufacture. We can thus establish a correlation between security scores and typosquatting domains.

Companies with lower security scores are less likely to take down such domains as part of their security programs. A high-value target like IT may still have many typosquatting domains, despite the efforts of their potentially stronger security programs.

Of course, three of these four industries are related, with significant overlap between IT, Semiconductors, and Other Electronics, comprising both software and hardware.

A ranking of these 40 top companies by their numbers of typosquatting domains makes this connection clearer and reveals a special emphasis on Semiconductors in particular. Semiconductor companies came in first, second, fourth, and fifth place on this list, with another two companies in the top 20.

IT companies came in third, eighth, ninth, and tenth place, also with another two companies in the top 20. Semiconductor companies not only scored lower in our sample; their industry is a top target for competitors such as China, which uses cyber espionage to gain competitive advantages.

Compromised Credentials

Compromised credentials, as revealed by our collection of data feeds from information stealing malware, serve as another security metric. Our platform tracks compromised credentials for each organization over the past four months and two years. When both timeframes were available, we averaged the two figures; otherwise, we used the one available figure.

The numbers of compromised credentials for each company ranged from 0 to 3100. 52 of the 150 companies (34.7%) had zero compromised credentials. The mean number was 106; the median was 5. If one excludes the 52 companies with zero compromised credentials and limits the data set to the remaining 98 companies, the mean number is 163; the median is 14. The much greater mean values, compared to the median values, indicates that this data set is “right-skewed.” In other words, the larger values at the higher end of the scale are inflating the mean values, whereas the median values are a more accurate representation of the data set.

The high-scoring Aerospace & Aviation sector was overrepresented among the companies with zero compromised credentials, with nearly twice as many companies in that subset than one would otherwise expect. This finding further establishes a rough correlation between security scores and compromised credentials. Companies with stronger security are less likely to experience such compromises and to remedy them if and when they do happen.

Further analysis of a subset of the 20 companies with 100 or more compromised credentials yielded more insights. Despite their higher security scores and perhaps because of their high value as targets, the IT sector had three times as many companies in this subset than one would expect. IT companies came in first, third, fourth, and sixth places on this list. Other Electronics was also overrepresented in this subset, with twice as many companies as one would expect.



Compromised Devices

Our IP Reputation security factor includes signs of possible malware infections or other device compromises in the past year. Our intelligence collection detects these compromises via sources such as sinkholes and honeypots. These findings include: infections with ransomware, information stealers, adware, and other types of malware; and the malicious repurposing of compromised devices, such as for attacks, scans, and use by the TOR anonymity network.

These findings do not necessarily indicate a full-scale breach of the affected organization. Indeed, they could mean little more than one infected or otherwise compromised device. They can nonetheless shed light on breaches that have not been reported yet, or that victims have not detected yet. A compromised device could be just the tip of the iceberg, or an initial access point from which a threat group moves laterally and expands its access across the network.

We found evidence of malware infections with payloads other than ransomware, adware, or information stealers at eight of the 150 companies in our sample, or 5.3% of it. Of note, the mean security score for those eight companies was 69, so that malware-infected subset had below-average security scores relative to our broader sample. Five of those eight companies were in either IT, Semiconductors, or Other Electronics, which is consistent with the above emphasis on those sectors in typosquatting and credential compromises.

We found evidence of adware infections at 17 of the 150 companies in our sample, or 11.3% of it. As with the malware-infected companies, the mean security score for these 17 companies was below-average relative to our overall sample, but less so (71). As with the malware-infected companies, a majority (10 out of 17) of them were in just one of three more heavily targeted sectors that we identified above: IT, Semiconductors, and Other Electronics.

We found two companies (1.3% of the sample) with compromised devices that attackers had maliciously repurposed for attacks on other devices outside those organizations' networks. Of note, both of these companies

were in the Textiles industry. They had a mean security score of 67, which is even more below-average relative to our broader sample and not surprising in light of the greater severity of this particular security metric. A compromised device is bad enough; it is even worse when defenders allow an asset under their protection to attack other infrastructure.

There was significant overlap between the companies with the three different types of compromises; 18 of the 150 companies in the sample (12% of it) had at least one of the three different types. Specifically, all but one of those compromised 18 companies had an adware infection. Only one company had just a malware infection but no detectable adware infections. In other words, from the perspective of our sample, almost all compromised companies have adware infections, which are less severe, but a large minority of those adware-infected companies (7 out of 17, or 41.2%) also have more severe malware infections or maliciously repurposed devices. Adware infections can thus serve as a red flag that there are other, more severe problems beyond the adware itself.

By the same token, the two companies with the maliciously repurposed devices were in that subset of seven compromised companies that had both malware infections and adware infections. Indeed, it is quite possible that their detectable malware infections were what enabled the malicious repurposing of the compromised devices on their networks in the first place.

That subset of seven companies with both malware and adware infections included one company with at least twice as many infections in both categories as the company with the second-largest number of infections in both categories. This "most infected" company was in the more heavily targeted Semiconductors industry and had an extremely low security score of 49.

Breach Histories

In General

16 of these 150 companies have had publicly reported breaches, yielding a breach rate of 10.7%. Three of these companies have had two breaches, yielding a total of 19. This percentage of breaches and this company/breach ratio are relatively low, especially in light of the low security scores that indicate widespread security problems. We suspect that underreporting may be a factor in this unexpectedly low figure. Media coverage of cyber attacks tends to focus on the U.S and, to lesser degrees, Europe and the more advanced and affluent economies of Northeast Asia.

Equally if not more unusual is the uneven distribution of breaches by industry/sector. There were no publicly reported breaches for four of the 10 industries/sectors: Semiconductors, Other Electronics, CX & BPO, and Transportation, Shipping, and Logistics. Given the value of the first three as targets and the often poor security postures described above, we further suspect that underreporting may be a factor in the lack of reported breaches for these industries/sectors.



By Industry

Nonetheless, the uneven distribution of breaches by industry/sector may nonetheless be more analytically useful for those industries/sectors with publicly reported breaches. Just two industries/sectors alone accounted for almost three-quarters (73.7%, or 14 out of 19) of the publicly reported breaches in our sample: IT and Pharmaceuticals & Medical Devices. Six of the 19 were in IT, and 8 of the 19 were in Pharmaceuticals & Medical Devices. Outside these two industries, there were only two publicly reported breaches in Automotive and one each in Aerospace & Aviation, Textiles, and Agriculture, Agribusiness, and Fertilizers. As if to reinforce the focus on those two industries, two of the three companies with two breaches were in Pharmaceuticals & Medical Devices, and the other company with two breaches was in IT.

Despite the above-mentioned concerns about underreporting and the potential implications thereof for our statistics, we believe that the concentration of breaches within those two industries does suggest an analytically valid trend. Our [previous reporting on trends in the U.S. and international markets](#) has indicated that those two industries are at higher risk than most others, so it would not be surprising if the same trend held true in India as well.

A Special Case: IT

The high concentration of breaches in the Indian IT industry (31.6%) may seem unexpected in light of that industry's unusually high security scores, as noted above. While security scores are a useful measurement of risk, they are not the only risk factors. Two other external factors are also at work: third-party risk and the choices of threat actors. A company's security is only as good as that of the vendors, suppliers, and other partners on which it relies. Companies with robust internal security can still experience third-party breaches via vendors, suppliers, and other partners with weaker security. Indeed, attackers may use third-party attack vectors against targets with stronger internal security specifically in order to bypass that stronger security.

The targeting preferences of threat actors are another factor. For example, Financial Services businesses often experience high breach rates despite equally high security scores simply because they are such popular targets. Many threat actors are willing to invest the greater resources and effort required to breach their stronger security because they are such desirable targets. We posit that IT businesses are popular targets for similar reasons that also pertain to third-party risk. IT companies are not only on the "receiving end" of third-party risk from their vendors, suppliers, and other partners. Compromised IT companies are almost nearly ideal third-party attack vectors for attackers to use against their customers, given the nature of the products & services that they provide and the sensitive access they often require.



Another Special Case: Pharmaceuticals & Medical Devices

The even higher concentration of breaches in the Pharmaceuticals & Medical Devices sector (a remarkable 42.1%) may seem obvious and expected at first glance. Readers in the U.S. and other Western countries may think of the broader Healthcare industry as a popular “soft” target for threat actors, particularly ransomware groups. We nonetheless excluded healthcare providers, such as hospitals and medical practices, from our definition of this industry because they are not part of India’s contribution to global supply chains, i.e. a physical product for export or a service rendered remotely for a foreign business. Healthcare providers like hospitals are responsible for much of the industry’s reputation as an easily and frequently exploited ransomware target.

Other sectors of the broader Healthcare industry, such as the pharmaceutical companies and medical device manufacturers that we have chosen for this study, nonetheless pose their own security challenges. Pharmaceuticals are an unusually IP-intensive business, making their developers and manufacturers high-value targets for threat actors that seek to compromise the IP that these companies or their partners may have spent massive sums of money to develop. The high value of this IP attracts not only more sophisticated criminals but even foreign intelligence services, such as those of China, which practices cyber IP theft in support of its own industries.

[Our analysis of the broader U.S. Healthcare industry](#) found that U.S. pharmaceutical companies had strong security scores even by U.S. standards, suggesting that they have made appropriately large investments in defense of their high-value IP. In contrast, the Pharmaceuticals & Medical Devices sector in India was the third-lowest scoring sector in our sample, just above Automotive and Textiles. An industry with both valuable data and weak security is a highly attractive target.

Medical device manufacturers pose a similar but less surprising problem. Despite the healthcare applications of their products, many of these companies are primarily manufacturers rather than healthcare companies. Their attack surfaces may resemble those of other manufacturers more than those of other healthcare companies. Manufacturers also tend to have lower security ratings, as we have seen elsewhere and noted above. Indeed, all five of the industries in this sample with below-average scores involved manufacturing, including Pharmaceuticals & Medical Devices.

Medical device manufacturers also had the lowest security scores within the broader U.S. Healthcare industry, [according to our previous study](#). This finding compounded previously existing concerns about medical devices as common sources of vulnerabilities in the attack surfaces of healthcare providers. It noted that relationships with the vendors themselves could pose additional third-party risk for the healthcare providers that maintain broader business relationships with the manufactures of the products that they use.



Third-Party Breaches

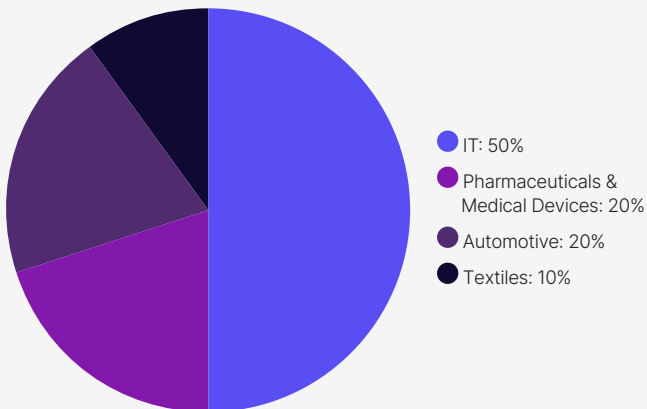
10 of the 19 breaches above (52.6%) were third-party breaches, in that either: a) breaches at these companies enabled the compromise of data or infrastructure for at least one other organization, or b); a compromise at another organization exposed data or infrastructure at these companies. In other words, it includes breaches in which the companies on our sample were both unwitting enablers, as well as those in which they were on “the receiving end” of third-party risk.

This rate of third-party breaches, indicating that a majority of breaches in our sample had third-party access vectors and/or repercussions, is relatively high. It is well above the global average of 35.5% that we established in [our Global Third-Party Breaches report earlier this year](#). Only a handful of our previous samples have had third-party breach rates higher than 50%, such as [the top 100 U.S. federal contractors](#) and [the global insurance industry](#).

The distribution of these third-party breaches by industry follows the risk profiles and targeting preferences described above. Five of the 10 third-party breaches, or exactly 50% of them, were in one industry: IT, which has the misfortune of frequently being both an unwitting enabler of third-party breaches of its customers, as well as a victim of third-party risk from its vendors. Pharmaceuticals & Medical Devices and Automotive both had two third-party breaches each. The remaining third-party breach was in the Textiles industry.



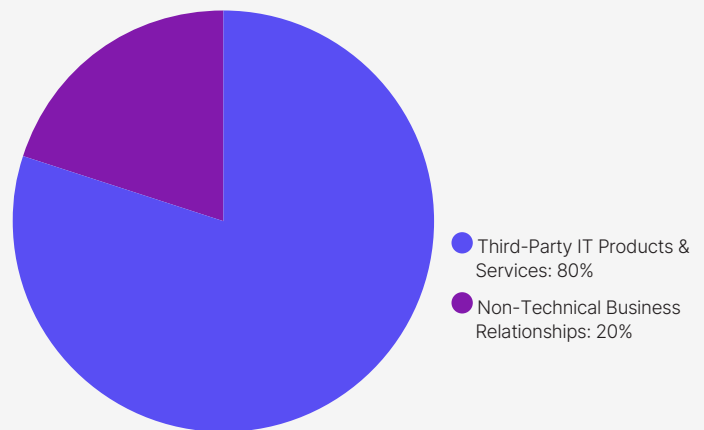
DISTRIBUTION OF THIRD-PARTY BREACHES BY INDUSTRY



Furthermore, even in those third-party breaches outside the IT industry, third-party IT products & services enabled eight of the 10 (80%) third-party breaches. Only two of the 10 third-party breaches occurred via non-technical relationships. Curiously, both of these breaches were in Pharmaceuticals & Medical Devices. One third-party breach involved a subsidiary and its parent company. Another third-party breach exposed information on the vendors of the compromised company, in an unusual reversal of typical third-party risk roles. Third-party risk is a two-way street; customers can also put their vendors at risk if they have access to sensitive information from the vendor, or if the vendors grant customers access to sensitive infrastructure.

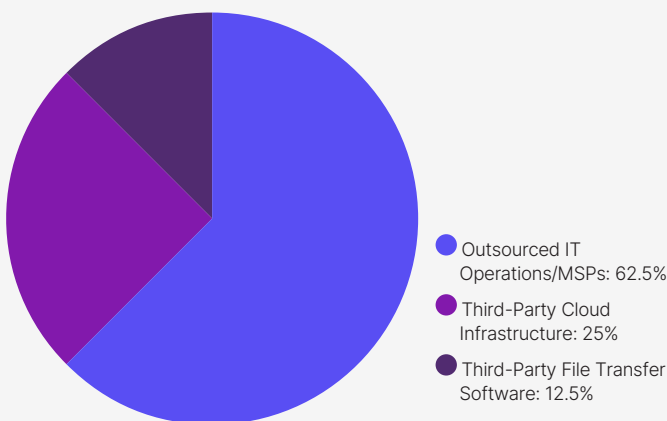
This emphasis on third-party IT products & services as top enablers of third-party breaches is consistent with our previous findings from U.S. and global samples. This figure can vary from as low as **46.75%** to as **high as 75%**, depending on the sample and other variables. 80% is the highest percentage that we have encountered thus far, although the relatively small sample size for third-party breaches may have inflated this figure somewhat.

TECHNICAL VS. NON-TECHNICAL ENABLERS OF THIRD-PARTY BREACHES



Further analysis of the third-party IT products & services that enabled these third-party breaches yielded more insights. Five of the eight breaches fitting this description (62.5%) involved the outsourcing of IT operations to third-party vendors or managed service providers (MSP). Two of the remaining breaches (25%) involved third-party cloud infrastructure. The other breach (12.5%) involved the exploitation of a zero-day vulnerability in third-party file transfer software.

TECHNICAL ENABLERS OF THIRD-PARTY BREACHES



Our prior reporting has often emphasized cloud infrastructure and file transfer software as top technical enablers of third-party breaches. They usually rank higher on the list than in this sample. MSPs and other IT operations outsourcing also often appear on our lists, but in lower ranks. The much greater emphasis on IT outsourcing in this case is likely due to the popularity of India as a place for foreign companies to outsource their business operations, including IT.

Ransomware Groups and Other Threat Actors

13 of the 19 breaches in our sample (68.4%) were ransomware attacks. Of note, five of those 13 ransomware attacks (38.5%) affected companies in the Pharmaceuticals & Medical Devices industry. The broader Healthcare industry has become a preferred target for ransomware operators mostly via attacks on healthcare providers, such as hospital systems or medical practices, which we did not include in our definition of this industry.

The components of this industry that we did include are nonetheless desirable ransomware targets for other reasons. The highly IP-intensive nature of the Pharmaceuticals business makes it particularly vulnerable to the threat of data disclosure. Both pharmaceuticals and medical devices involve manufacturing, a field that is often another preferred target for ransomware operators due to the opportunity to put more pressure on victims to pay by disrupting victims' manufacturing operations.

The time-sensitivity of the often life-saving products & services of the broader Healthcare industry are another reason for its popularity as a ransomware target. In the classic case of hospitals or other medical practices, outages due to ransomware attacks can delay time-sensitive care or treatments for patients whose lives or health are in jeopardy.

In the case of Pharmaceuticals, this time-sensitivity was applicable to them at least during the COVID-19 pandemic, when many companies were rushing to develop, manufacture, and distribute COVID-19 vaccines as soon as possible. [An Indian pharmaceutical company in our sample suffered a ransomware attack that delayed its planned clinical trials for a COVID-19 vaccine.](#)

Five of these 13 ransomware attacks (38.5%) were also third-party breaches. By the same token, six of the 10 third-party breaches (60%) were also ransomware attacks. We have seen this same close correlation and extensive overlap between ransomware attacks and third-party breaches in previous U.S. and global samples, so it was not a surprise to see it in this Indian sample too.

There are two reasons for this correlation and overlap. Third-party attack vectors often enable ransomware groups to scale their operations and infect as many victims as possible with little or no extra input.

Only some victims pay ransoms, so ransomware groups have an incentive to infect more victims. On the other side of the third-party risk equation, the extortionate disclosures of data compromised in many ransomware attacks often deliberately include sensitive information on vendors, customers, and other partners or third parties specifically in order to inflict maximum pain on the original victims by damaging their external relationships.

12 of the 19 breaches in our sample were attributable to named threat actors. 10 of those 12 attributable breaches (83.3%) were attributed to ransomware groups. While this high proportion does reflect the dominant position of ransomware groups in the criminal threat landscape, it also reflects the often greater ease of attributing ransomware attacks in particular to a named group.

In any event, only one ransomware group appeared more than once on this list: C10p. This prolific group is a textbook example of the correlation between ransomware and third-party attack vectors. C10p often infects large numbers of victims at once by exploiting vulnerabilities in third-party software, such as file transfer software. The effectiveness of this strategy is probably why C10p is the only ransomware group to appear on our list more than once.

The other two threat actors were a non-ransomware criminal and the Chinese cyber espionage group APT10. Chinese cyber espionage deserves special consideration among state-sponsored threats to India due to both geopolitical and economic competition between these top two Asian powers.

In particular, India's emergence as a key contributor to global supply chains, particularly in industries such as IT, Semiconductors, Other Electronics, and Pharmaceuticals & Medical Devices, threatens China's global economic ambitions and its dominance of key supply chains. Nonetheless, the specific breach in question was part of a [global campaign in which APT10 used cloud services as a third-party access vector to breach major IT companies around the world.](#)

Recommendations

1. Use This Paper to Calibrate Your Third-Party Risk Management (TPRM) Program

This research has many findings that TPRM teams can use to adjust their coverage of Indian suppliers, based on industry and the various types of security issues, among other variables. For example, a U.S. or European aircraft manufacturer that has Indian suppliers in both the IT and the Aerospace & Aviation industries should subject the former to much greater third-party risk scrutiny than the latter, given our above findings and despite the former's higher security scores. Patching Cadence issues at Indian suppliers deserve greater emphasis than they would at vendors in other markets, given the more pervasive Patching Cadence problems we have identified.

2. Prioritize TPRM for Third-Party IT Products & Services

Third-party IT products & services from India deserve higher levels of cyber risk scrutiny in particular, given both: a) the global salience of such products & services as enablers of third-party breaches worldwide, and b): the extensive targeting of and compromises at top Indian IT companies, which occur at high rates despite those companies' relatively high security scores. The extensive foreign outsourcing of IT operations to Indian companies gives threat actors enormous opportunities to compromise global companies via their Indian IT vendors.

3. Require Breach History Disclosures from Suppliers

Breach history disclosures should be required for all vendors, but they may be even more important for Indian suppliers due to potential underreporting of Indian breaches by news media. Prior breach histories not only yield insights into a company's security posture and its weaknesses; they may also shed light on future breach risks. Compromised credentials and network reconnaissance from a breach may plant the seeds of future breaches when they circulate in online criminal communities. Indeed, some attackers maintain access to and return to exploit previous targets further. Some ransomware operators try to extort second ransom payments from victims that have already paid. A company that is known to have paid in the past is a more desirable target for future extortion because it has demonstrated a willingness to pay.

4. Require Vendors to Run Their Own TPRM Programs

Your vendors and suppliers have their own vendors and suppliers. Your vendors and suppliers incur third-party cyber risk from those vendors and suppliers of theirs, just like your company incurs third-party cyber risk from them. Those third-party risks to your vendors and suppliers become your own fourth-party risks. Require your vendors and suppliers to run their TPRM programs to prevent their third-party cyber risks from becoming your fourth-party breaches.

5. Remain Alert for "Canaries in the Coal Mine" and Other Red Flags

Some security signals and metrics deserve more attention or consideration than others. In the case of this sample, we saw that poor Patching Cadence was one of the most common poor security practices that correlated with higher breach count across industries. We have observed in other research that companies scoring lowest in this security factor tend to have weaker security in general. It is thus not surprising that Patching Cadence was such a salient problem in this unusually low-scoring Indian sample. If you have an Indian supplier with significant Patching Cadence issues, make that supplier a high-priority focus for further scrutiny in general, beyond the specific Patching Cadence issues themselves. Such companies are likely to have other, equally or more severe problems. By the same token, a company with an adware infection may also have other compromises of a more severe nature on its network, as we saw in this Indian sample.

Methodology

We identified 10 industries and sectors in which Indian businesses either make key contributions to global supply chains or, in the case of the last one, facilitate such contributions by enabling physical Indian products to reach foreign markets as exports.

1. Semiconductors
2. Other Electronics
3. Automotive
4. Aerospace & Aviation
5. Pharmaceuticals & Medical Devices
6. Information Technology (IT)
7. Customer Experience (CX) & Business Process Outsourcing (BPO)
8. Textiles
9. Agriculture, Agribusiness, and Fertilizers
10. Transportation, Shipping, and Logistics

For each of those 10 industries and sectors, we identified 15 companies that were among India's top exporters or service providers for foreign businesses and consumers or otherwise had some strategically important role in India's contribution to global supply chains. For each of these 150 companies, we compiled and analyzed the following data points from our platform:

- Overall security score
- The one of 10 cyber security risk factors in which each company scored the lowest
- The numerical value of the security factor in which each company scored the lowest
- The one individual security issue that had the most negative impact on its score
- Any publicly reported data breaches for this company, third-party or otherwise
- The nature of the relationship that caused any third-party or fourth-party breaches
- Any threat actors to which breaches were attributed, particularly ransomware groups
- Any evidence of malware infections or compromised machines on a company's network
- Numbers of leaked credentials and suspected typosquatting domains for each company.



To learn more and create
your free account, visit
SecurityScorecard.com

ABOUT SECURITYSCORECARD

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on [LinkedIn](#).



SecurityScorecard.com
info@securityscorecard.io