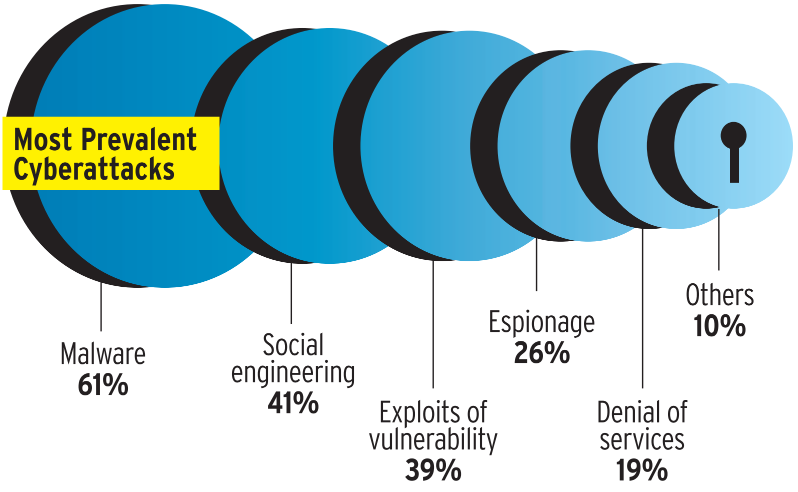
RAJ VERMA

Security Breach

Even as online frauds become more and more vicious, companies and law enforcement agencies seem to be losing the battle. **By DIPAK MONDAL**

Last year, Saudi Aramco, which buys naphtha from ONGC, received an e-mail asking it to deposit ₹100 crore for its latest purchase in a new bank account with Bangkok Bank Public Company Ltd instead of the usual State Bank of India account. The Saudi Arabia-based company did so in September. Same month, it deposited another ₹97 crore in the new account for the same deal. But ONGC never got the money. On October 7, when it got an e-mail from Aramco about the transfer, it knew something was wrong. It had been defrauded by cybercriminals through a trick called the man-in-the-middle in which a person, probably an insider, writes an e-mail on behalf of the company for re-directing a payment to an account operated by the fraudsters themselves. This person knows the e-mail id of the buyer. He may also know the e-mail password of the seller. Even if he does not know the latter, he may create an e-mail id similar to the seller's. In ONGC's case, for instance, the fraudsters tweaked the e-mail id from *patel_dv@ongc.co.in* to *patel_dv@ognc*.co.in. It is difficult to detect the difference at first glance. Text and e-mail messages sent to the ONGC spokesperson were not answered.



Source: KPMG Cybercrime Survey 2015 of 250 executives (chief investment officers, chief risk officers, and chief operating officers); figures add up to 100 per cent-plus as each question had more than one answer

In another case, a hacker spoofed the e-mail id of Flipkart Co-founder Binny Bansal and sent mails to Chief Financial Officer Sanjay Baweja asking him to transfer $80,000 to his bank account. Though a company statement says the spoofing was detected and a report filed with the police, the incident shows that cybercriminals are not scared of going after the big guns, too.

Incidents handled by CERT-IN

	2012	2013	2014
Spam	8,150	54,677	85,659
Website Intrusion & Malware Propagation	4,591	5,265	7,286
Virus/Malicious Code	3,149	4,160	4,307
Others	2,417	3,484	3,610
Network Scanning/Probing	2,866	3,239	3,317
Phishing	887	955	1,122
Total	22,060	71,780	105,301

Source: CERT-IN, a nodal agency that deals with cyber security threats

These incidents are not one-off. There has been an estimated five-fold rise in the number of reported cybercrimes in India between 2012 and 2014. What is worrying is that most companies in the country are not up to the task of protecting themselves. Law enforcers, too, fail as perpetrators usually operate from foreign shores and use 'jurisdictional arbitrage' — which means operating from jurisdictions with lax laws such as Africa and Eastern Europe — to get away.

Even if the country where the fraudsters stay has sound cyber laws, it takes enormous time and effort to ensure coordination with its enforcement agencies. In most cases, before the case reaches its logical conclusion, both the money and the evidence are gone. Experts and enforcement agencies say there is 10 per cent chance of recovering money that has gone out of the country.

Fraud Surge

There has been a steep rise in the number of cyberattacks and frauds in the past couple of years. Though we do not have the exact number of reported cases, one way to establish the point is cases handled by CERT-IN, a government nodal agency that deals with cyber security threats. The number of cases handled by it rose almost five times from 22,060 in 2012 to 1,05,301 in 2014. Of course, not all cybercrimes are financial frauds; they also include crimes such as defacement of website, insult to modesty of women and personal revenge. According to the National Crime Record Bureau, the number of reported cybercrimes rose 69 per cent from 5,693 in 2013 to 9,622 in 2014. Of these 9,622 cases, 18 per cent, or 1,736, related to greed/financial gain, and 495 related to fraud/illegal gain.

VIVAN MEHRA

Karnika Seth, Cyber Law Expert, Seth Associates

> "Hackers are using a lot of new tools such as key-loggers that help them know what you are typing on your computer. These tools can be so sophisticated that you would not know that your computer has been infected"

New Tools

The bad news for law enforcers is that the attackers are using more and more sophisticated tools to break into cyber security systems. Their basic methods may have remained the same for years but they have been continuously evolving new strategies to stay ahead of their prospective victims.

For instance, the man-in-the-middle attack, faced by ONGC, is one of the oldest tricks. Earlier, it required an insider. But now, criminals are increasingly using a trick called 'social engineering' to get classified information from employees, for example by posing as the company's IT helpdesk staff. The information stolen may be password, date of birth, email id, etc, that can be used to carry out the fraud. Phishing is another form of social engineering. In it, the attacker, through an email or a website, gets personal information by posing as a representative of an organisation.

Another common attack that large companies, especially those in the services sector, face is denial-of-services. Here, multiple compromised systems are used to crash a website by doing more logins than it can handle. The attackers demand a ransom for backing off. Targets could be banks, e-commerce portals or travel websites. For instance, on January 15, HSBC UK's online services were halted for a couple of hours due to such an attack. It is not known if a ransom was sought. In similar attacks in India reported in media, last year, hackers took control of computer systems of three banks and a pharma company and demanded ransom in bitcoins, a digital currency whose unit is valued around ₹28,000.

Another form of cyberattack is corporate espionage. Here, sophisticated software is used to get access to a computer network and get confidential information such as sensitive data and intellectual property assets. This information can be sold to competitors. The hacker may also seek a hefty sum for not leaking the information. Last year, two Indian companies were forced to pay millions after attackers who hacked into their system got to know that they were involved in activities that violated the law of the land.

"Hackers are using a lot of new tools such as key-loggers that help them know what you are typing on your computer. These tools can be so sophisticated that you would not know that your computer has been infected. Sometimes even the best of anti-viruses cannot detect key-loggers," says Karnika Seth, a cyber law expert at law firm Seth Associates.

Losing battle

Suprabhat N.M., who leads the forensic services practice at Protiviti India, a global consulting firm, was entrusted with investigation into a case where a Coimbatore-based textile exporter was defrauded. One of the company's Brazilian buyers was coaxed by cybercriminals into transferring a payment to a bank account in Poland instead of the regular Singapore account. Suprabhat's investigation helped the company track the local person who unwittingly helped the criminals by parting with the company's e-mail id and client details. His team could not recover the money. He says it is difficult to even trace the account after the fraud has been committed.

Suprabhat says there were 10 more such cases in Coimbatore alone around that time. Usually, it is the smaller companies that fall prey to such tricks, as they do not have the resources to build robust cyber security systems.

Arpinder Singh, Partner & National Leader, E&Y, says, "In cyber fraud cases where money has gone out of the country, our experience says there's less than 10 per cent probability of recovery. At times it's not worth pursuing the case as you have to do it across jurisdictions, sometimes in different continents. Most of the time companies give up."

A report by computer security software company McAfee puts annual loss to the global economy due to cybercrime at $400 billion in 2014. This was 0.8 per cent of global gross domestic product or GDP. The report puts India's loss at 0.21 per cent of GDP (low as per the report), though many other reports have warned the country about these losses. A 2013 Symantec report had called India the ransomware capital of Asia Pacific.

The conviction rate also paints a bleak picture. According to the National Crime Records Bureau of India, out of 9,622 cases registered

COMMON CYBERCRIMES COMPANIES FACE

MAN-IN-THE MIDDLE ATTACK: The attacker gets in between two parties – the company and its clients – by impersonating as the former and diverts payments to his account.

EXAMPLE: ONGC lost ₹197 crore when cybercriminals duplicated its official e-mail address and used it to convince a Saudi Arabia-based client to transfer money to their account.

DENIAL OF SERVICE: Multiple systems are used to target a website by exceeding the limit of concurrent users it can handle. The site crashes and resumes only after the company pays the criminals.

EXAMPLE: HSBC UK's website faced such an attack in January this year. Customers could not access services for hours

PHISHING/SPOOFING: Creating a forged email id or IP address and impersonating to get sensitive information that can be used for monetary gains

EXAMPLE: Cybercriminals recently spoofed the e-mail id of Flipkart Co-founder Binny Bansal and sent e-mails to the CFO, Sanjay Baweja, asking him to transfer $80,000 to their bank account.

CYBER ESPIONAGE: Hackers gain access to a network and get confidential information. They can then use the information for unauthorised debits from bank accounts, extortion, etc.

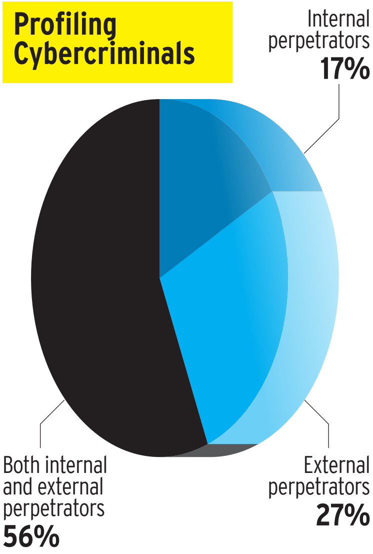
EXAMPLE: Last year, two Indian companies were forced to pay millions in ransom to stop hackers from revealing information about their involvement in activities that were against the law of the land.

in 2014, just 0.7 per cent, or 72, ended in conviction.

These are just the reported cases. The number of unreported cases would be much more as a lot of frauds involving companies are not reported due to fear of loss of reputation. "A bank would not report a breach unless it is big. Why would it risk its image by telling everyone that its security has been breached?" says a cybercrime expert with the Enforcement Directorate.

India's laws also do not require companies to report these incidents, says Nandkumar Saravade, CEO, Data Security Council of India, a premier industry body on data protection set up by NASSCOM, the information technology industry's representative body.

Even when complaints are lodged, it is rare for criminals to be brought to justice. "The attackers are always remote. They use jurisdictional arbitrage. They know which geographies have lax laws, and that law enforcement agencies will focus only on problems in their jurisdictions. If someone is quietly operating from one area and attacking someone in another, law enforcement agencies in the latter have no reason to go after him. And the coordination among enforcement agencies of different states, forget about nations, is inadequate," says Saravade.



Source: KPMG Cybercrime Survey 2015

Anyesh Roy, DCP, Cyber Cell, Economic Offences Wing (EOW), Delhi Police, says in most cases money is diverted to a foreign country. "If the country where the money has been siphoned off has a sound law and order system, the case can be pursued there. We have seen that the enforcement agencies of such countries do respond to our queries even if the response may come a little late."

However, the response may not be adequate. Often, coordination takes so long that both evidence and money disappear. "The traditional mechanism for international cooperation is the Mutual Legal Assistance Treaty or MLAT. But the process under MLAT takes a long time — at least one year and more. But in cybercrime, if you don't act fast, the evidence is gone. MLAT is not of much use," says Saravade.

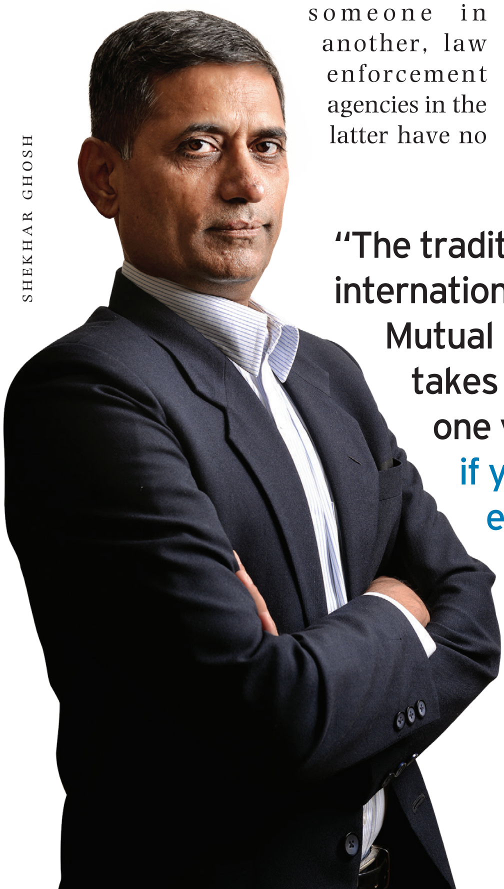
In order to expedite the flow of information and act quickly, a Convention on Cybercrime was formed in 2001. Many, including the US, European Council, Canada, Japan and South Africa, joined. India is yet to become a signatory. "Joining it has been one of the demands of industry. Without this, the cooperation we get is rudimentary. This works in favour of criminals," says Saravade.

While international coordination remains a far cry, are local law enforcement agencies equipped to deal with cybercrime? Recently, the Delhi Police said that each police station would have one sub-inspector and two constables to help the station house officer in cybercrime cases.

"We have a cyber lab where we have hired people from technology background (B Tech and MCA). Besides, we take the services of CERT-IN software systems. Unofficially, of course, we also take help from technology guys," says Roy of Delhi Police's EOW.

But Delhi Police is probably one of the most well-equipped police forces in the country. In other states, things are much worse. "Earlier, the police (in other states) were setting up cybercrime cells at district headquarters levels. That time is gone. We now need to go to the police station level," says Saravade. ◆

@dipak_journo



SHEKHAR GHOSH

"The traditional mechanism for international cooperation, the Mutual Legal Assistance Treaty, takes a long time– at least one year. But in cyber crime, if you don't act fast, the evidence is gone"

Nandkumar Saravade
CEO, Data Security Council of India