The Asian AGe October 24, 2016

CYBER THREATS

Sebi wants more safeguards

Data breach forces the market regulator to rethink security plan

New Delhi, Oct. 23: Markets regulator Sebi is mulling a greater push to put in place strong safeguards against cyber threats to bourses, brokerages and other entities, amid concerns over the largest-ever banking data breach wherein 32 lakh debit cards are feared to have been 'compromised'.

The regulator will also look at the best global practices in this regard including through inputs from the regulatory authorities in advanced markets, while consultations will be held with government entities as well as with the information technology and cyber security experts, a senior official said.

While Sebi, which is mandated to regulate stock exchanges, clearing corporations, brokerages, portfolio managers, fund houses, rating agencies and a host of other entities in the capital market space, is already in the process of appointing a chief IT security officer to oversee various initiatives aimed at protecting the marketplace from cyber threats.

The regulator has further beefed up its efforts and wants to fast-track the work on a new and stronger policy framework in the areas of cyber security in the wake of the recent suspected compromise of 32 lakh debit cards, the official said.

The matter assumes significance as the entire marketplace is closely linked and a cyber security threat in one segment of the capital markets can prove to be disastrous for other segments as well. The official also said the regulator is looking to beef up its own surveillance and risk management systems, as also that of the market infrastructure entities to check any cyber threats, while various intermediaries would also be asked to beef up.

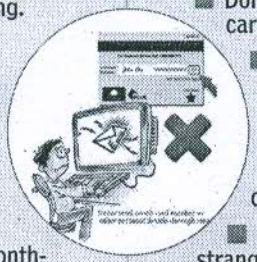
— *PTI*

ATM GUIDELINES

certin — Handling Cyber-crisis Security Incidents

DO's

- Before you use an ATM, please ensure that there are no strange objects in the insertion panel of the ATM.(to avoid skimming)
- Shield the ATM pin number during transaction. Don't carry the transaction receipts along.
- Please change your ATM PIN once in every 3 months as advised by banks.
- Keep your credit card receipts to guard against transaction frauds, check your receipts against your monthly statement.
- Only carry around credit cards that you absolutely need.
- Shred anything that contain your credit card number written on it. (bills)



DON'Ts

- Don't accept the card received directly from bank in case if it is damaged or seal is open.
- Don't write your PIN number on your credit card.
- Don't carry around extra credit cards that you rarely use.
- Don't disclose your Credit Card Number/ATM PIN to anyone.
- Don't hand over the card to anyone, even if he/she claims to represent the Bank.
- Don't get carried away by strangers who try to help you use the ATM machine.
- Don't use the ATM machines if the device is not in good conditions.
- Don't transfer or share your account details with unknown/non validated source.

INDIA ALWAYS ON THE RADAR OF CYBER CRIMINALS

AGE CORRESPONDENT
NEW DELHI, OCT. 23

The debit/ATM card frauds as detected by some of the largest banks were waiting to happen, as India has been on the radar of the global cyber criminals who hack into the computer servers using the malware, putting the entire financial structure at huge risk, said an industry study.

According to a recent Assocham-Mahindra SSG, India was the third biggest target for these hackers after the US and Japan. "Assocham has been continuously sensitising the government, RBI and the banks against the unfolding cyber risks," Assocham secretary general D. S. Rawat said. He said the study published recently pointed out that India has become a favourite hunting ground for global hackers and criminals.

It said "There has been a sixfold increase over the past three years."

October 23, 2016

The Statesman

ASSOCHAM IN THE NEWS

Bank card fraud was waiting to happen, says Assocham study

statesman news service

NEW DELHI, 22 OCT: The credit/debit/ATM card fraud as detected by some of the largest banks was waiting to happen as India has been on the radar of global cyber criminals who hack into computer servers using malware, putting the entire financial structure into a big risk, an Assocham-Mahindra SSG joint study had forewarned.

"Shocked that we are by such large volume of frauds forcing most of the big banks to recall their swiping cards resulting in not only huge financial losses but also raising a question mark on our cyber security, Assocham has been continuously sensitising the government, RBI and the banks against the unfolding cyber risks," the chamber Secretary General Mr DS Rawat said.

He said an Assocham-Mahindra SSG study published recently pointed out that India has become a favourite hunting ground for global hackers and criminals. In fact, according to this study, India was the third biggest target for these hackers after the US and Japan.

A rapid increase in the use of computers and the emergence of the Internet in particularly in the last few decades has led to the evolution of cyberspace. Cyberspace is borderless and anonymous due to which it becomes difficult to actually trace the origin of any kind of cyber attack. The study had noted that mobile frauds are an area of concern for companies as 35-40% of financial transactions are done via mobile devices and this menace is expected grow to 60-65% by 2017.

Credit and debit card fraud cases top the chart of cyber crimes. There has been a sixfold increase in such cases over the past three years. According to the report's data, about 42% complaints of online banking related to/credit/debit card fraud followed by Facebook - related complaints (31%) (morphed pictures/cyber stalking/cyber bullying). Other major cyber complaints were cheating through mobile (12%), hacking of e-mail ID (10%), abusive/offensive/obscene calls and SMS (5%), and others. These attacks have been observed to be originating from the cyberspace of a number of countries including the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE, the report said.

Andhra Pradesh, Karnataka and Maharashtra have occupied the top three positions when it comes to cyber crimes registered under the new IT Act in India.

Phishing attacks on online banking accounts or cloning of ATM/debit cards are common occurrences. The increasing use of mobile/smartphones/tablets for online banking/financial transactions has also increased the vulnerabilities to a great extent. The maximum offenders came from the 18-30 age group, the report added.

"Internet frauds alone have cost India a whopping 4 billion $ (about Rs 24,630 crore) in 2013 as cyber criminals are using more sophisticated means like ransom ware and spear-phishing," the report said.

During 2011, 2012, 2013 and 2014 a total of 21,699, 27,605, 28,481 and 36,554 Indian websites were hacked by various hacker groups worldwide. In addition, during these years, a total number of 13,301, 22,060, 71,780 and 95,189 security incidents, respectively, showing a sharp increasing trend, it said.

There is urgent need for having public-private-partnership (PPP) in cyber security for protecting critical online data and creating awareness amongst the public, the report said. Internet has many stakeholders and the government is involved in terms of making laws and the private sector is involved in creating hardware, software and so on., the report said, adding this can't be seen in an isolated manner which is why PPP model is important. The fifth domain warfare is real and expanding at a rate which is more concerning, ISIS use of cyber space for expanding its base and support is glaring example of this, it pointed out.

Cyber attacks around the world are occurring at a greater frequency and intensity. Operating securely in the cyber environment is among the most urgent issues facing the government, industry and individuals. It is important to take proactive measures rather than reactive methods as building safe environments will always be the best line of defence against rising cyber crime. 'Safety first through security by design' should be the motto. Security by design ensures reduction in overall cost to the business and increases the efficiency of the system by making it robust and secure, the report said.

The government and regulators should develop comprehensive cyber security policies and frameworks from the perspective of incentives, tax breaks and technological development, it added.

ASSOCHAM IN THE NEWS

Rashtriya Sahara

October 24, 2016

वित्तीय तंत्र के लिए खतरनाक है साइबर अटैक

■ नई दिल्ली।

उद्योग एवं वाणिज्य संगठन एसोचैम ने कुछ बैंकों के क्रेडिट/डेबिट कार्डों के साथ हुई गड़बड़ी को पूरे वित्तीय तंत्र के लिए खतरनाक बताते हुए कहा है कि भारत लंबे समय से वैश्विक साइबर अपराधियों के निशाने पर है और यह होना ही था।

एसोचैम और महिन्द्रा एसएसजी के संयुक्त अध्ययन में कहा गया है कि साइबर अपराधियों ने मालवेयर का इस्तेमाल करके कम्प्यूटर सर्वरों को हैक किया और वित्तीय तंत्र को बड़े खतरे में डाल दिया।

उसने कहा, अधिकांश बड़े बैंकों द्वारा कार्डों का वृहद स्तर पर वापस लिया जाना दुखद है। इससे न केवल वित्तीय नुकसान हुआ है बल्कि इसने हमारी सुरक्षा व्यवस्था पर भी सवालिया निशान लगाया है। एसोचैम ने कहा कि भारत वैश्विक हैकरों और साइबर अपराधियों की दिलचस्पी का केन्द्र बन गया है। ■ वार्ता

एसोचैम की रिपोर्ट

■ लंबे समय से साइबर अपराधियों के निशाने पर था भारत

■ 2013 में नेट फ्रॉड से हुआ था ₹24,630 करोड़ का नुकसान

■ देश में आंध्र प्रदेश, कर्नाटक और महाराष्ट्र साइबर आपराध के केंद्र

कितनी बार हैक हुई भारतीय वेबसाइट

वर्ष	संख्या
2011	21699
2012	27605
2013	28481

अमेरिका, यूरोप, ब्राजील, तुर्की, चीन, पाक, बांग्लादेश और यूएई में साइबर अपराधी ज्यादा

Rajasthan Patrika October 24, 2016

कार्ड फ्रॉड सिस्टम के लिए खतरनाक है: एसोचैम

नई दिल्ली @ पत्रिका. उद्योग एवं वाणिज्य संगठन एसोचैम ने कुछ बैंकों के क्रेडिट/डेबिट कार्डों के साथ हुई गड़बड़ी को पूरे वित्तीय तंत्र के लिए खतरनाक बताते हुए कहा है कि भारत लंबे समय से वैश्विक साइबर अपराधियों के निशाने पर है और यह होना ही था। एसोचैम और महिन्द्रा एसएसजी के संयुक्त अध्ययन में कहा गया है कि साइबर अपराधियों ने मालवेयर का इस्तेमाल करके कम्पयूटर सर्वरों को हैक किया और वित्तीय तंत्र को बड़े खतरे में डाल दिया।

एसोचैम ने कहा, 'अधिकांश बड़े बैंकों द्वारा कार्डों का वृहद स्तर पर वापस लिया जाना दुखद है। इससे न केवल वित्तीय नुकसान हुआ है, बल्कि इसने हमारी सुरक्षा व्यवस्था पर भी सवालिया निशान लगाया है। एसोचैम ने कहा कि भारत वैश्विक हैकरों और साइबर अपराधियों की दिलचस्पी का केन्द्र बन गया है। भारत अमेरिका और जापान के बाद इन हैकरों का तीसरा बड़ा निशाना बन गया है। रिपोर्ट में कहा गया कि पिछले कुछ दशक में कम्पयूटरों के इस्तेमाल में बड़ी तेजी तथा इंटरनेट के विस्तार से साइबरस्पेस विकसित हुआ है।