Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)

Target Inc Ruling: An Inflection Point for Cyber Vigilance

Wg Cdr Ashish Gupta
Research Fellow, CAPS

The financial institutions and banking industry stand at the cusp of changes that are transforming the way they function in cyber space. In the financial domain, technology is both an enabler and a business driver, facilitating growth in extending financial services to masses. By leveraging the phenomenal growth of IT, mobile and communication network, financial services have become efficient, accessible and affordable, increasing their outreach and impact on the lives of people. This has also made it necessary to seek a paradigm shift in areas of security, protection of confidential information, service delivery and consumer rights. As cyber criminals continue to develop and advance their techniques, they have become selective in choosing their targets and exploiting their vulnerabilities. While certain tenets of cyber crime share a converging pattern with conventional form of criminality, it has a distinct character, unprecedented and unparalleled in the annals of criminology; one that requires different mechanisms to deal with it.

The judiciary and law enforcement agencies are grappling with the enormity of challenges posed by criminals operating in cyberspace. Cyber forensics is still a fledgling branch of criminology, trying to find its bearing and effectiveness in the murky and unforgiving cyber landscape. [1] In an incident, which saw an ensuing legal battle between US discount retailer Target Corporation and various banks, a District Judge in Minnesota gave a landmark verdict, which may serve as a point of reference for issues related to accountability and apportionment of responsibilities for future legal battles related to

cyber operations. A retailer heavyweight, Target Corporation is the second largest retailing company in US after Wal-Mart Stores. A fortune 500 company, it was ranked 36th in the year 2013 and is headquartered in Minneapolis, Minnesota. It claims to offer exquisite shopping experience at competitive discount prices and outstanding value. Its stores across the US are flocked by millions of Americans year around with many fold increase in numbers during Thanksgiving. [2] In November last year, in a highly ingenious and inventive way, a week preceding Thanksgiving, someone installed a malware in Target's security and payments system designed to record the details of every credit and debit card used at company's 1,797 U.S. stores. In the spirit of festivity, when an unsuspecting customer pays for the Christmas gifts, the malware kicks in, captures shopper's credit card number and stores it in one of the company's server, compromised and controlled by the hackers. Such information is a treasure- trove for unscrupulous **black-marketers, who** could sell this to the highest bidder for producing fake credit cards.

Six months prior to this, the company had installed a 1.6 million US dollar malware detection software, made by the computer security firm FireEye, a company of formidable repute in the field of computer security with equally impressive lists of customers including the CIA and the Pentagon. However, during internal investigation, it was admitted by a number of Target employees, who spoke on the condition of anonymity, that the technology gave enough warning signs which went unheeded until hackers had already stolen credit and debit card information for 40 million customers from its system.

At least 90 lawsuits have been filed against Target in US courts by customers and banks for negligence and compensatory damages. [3] Customers, represented by law firm Hagens Berman Sobol Shapiro LLP, alleged that Target Inc ignored warnings about its point-of-sale (POS) system vulnerability towards attack. The lawsuit also claims that Target failed to comply with the standards for security, such as storing of CVV codes of credit cards, a practice long banned. The banks which issued the credit and debit cards suffered major financial losses from this security breach at Target. In their efforts to recoup losses, the bank also filed law suit against Target claiming that the company had failed in securing its computer systems, allowing hackers to breach the system security. [4]In its

defence, the retailer's lawyer argued that the company was not legally accountable to the banks as the payments made through cards, were processed through third-party intermediaries. The claims of banks, that Target had a duty to protect their interest, were also refuted on the grounds that applicability of these claims could only be binding if framed within the legal provisions. The lawyer argued that since no such legal provisions existed, Target should be absolved of any liability to the lenders and case needed to be summarily dismissed.

As a general prevailing practice, the financial institutes are left to shoulder the monetary losses resulting from an episode of hacking. In this case, it cost a staggering 400 million US dollars to various banks just to replace the compromised cards with new cards. In addition, banks incurred expenditure on account of monitoring the cases due to fraudulent use of stolen cards and reimbursement made to the victimized customers. The five major banks including- Umpqua Bank in Roseburg, Oregon, Mutual Bank in Whitman, Massachusetts, Village Bank in St. Francis**, Minnesota**, CSE Federal Credit Union in Lake Charles, **Louisiana** and First Federal Savings Bank in Lorain, Ohio, which were affected by Targets' inability to fully secure its system, formed a loose union for seeking monetary compensation for damages suffered.

On 04 December 2014, a US District judge in Minnesota rejected Targets' plea to dismiss lawsuits by the banks. The ruling will bring some clarity in apportioning the responsibilities in the cases related to data breaches. Though the lawsuit is still continuing, a loose consensus is building up in the legal community that this early ruling could have long and widespread ramifications on the outcome of future cases of data breaches. The ruling makes it clear that banks cannot be held hostage on account of negligence on the part of a complacent company, of its computer security system. The judge took cognizance of charges against Target for ignoring security software alerts and disabling some of its security features, which is tantamount to an act of gross negligence. Judge Magnuson remarked that, "Imposing a duty on Target in this case will aid Minnesota's policy of punishing companies that do not secure consumers' credit and debit card information." He further added that, "Although the third-party hackers' activities caused harm, Target

played a key role in allowing the harm to occur." The ruling by the judge on the motion to dismiss does not end the legal battle and with no clear winners, the case will proceed to the next phase, offering Target another shot at arguing its case emphatically. However, if the current ruling is any indication, the scales are weighed heavily against Target.

In the past, the liability issues in data breach cases were governed by interpreting various provisions in contracts between users, banks, commercial ventures accepting the credit cards and credit card companies. This ruling will provide a legal framework to apportion the responsibility for monetarily compensating an aggrieved party associated with a hacking incident. As such, in cyber space, the issues related responsibility, **attributability, and accountability are deeply intertwined and complex.** The shroud of anonymity behind which cyber-criminals operate has made the process of establishing the identity of transgressors an arduous one. Attribution is first step in assigning responsibilities and seeking legal recourse. The present legal system and enacted laws **find themselves** in a **cul**-de-sac of cyber space and fail to act as a deterrent to cyber-criminals. For rule of law to be effective, it must ensure that the costs of non-compliance exceed the costs of compliance. The outcome of this incident needs to be monitored closely as it may provide a tangible recourse for affixing the responsibilities.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

End Notes

[1] "Target (TGT): Millions Could Be Affected By Credit Card Data Breach, Payment Info Theft ", at http://www.ibtimes.com, accessed on 25 Nov 14

[2] "Target-missed-alarms-in-epic-hack-of-credit-card-data", at http://www.businessweek.com/articles/2014-03-13/ accessed on 25 Nov 14

[3] "Target-Data-Breach", at http://www.hbsslaw.com/cases-and-investigations/cases, accessed on 25 Nov 14

[4]" Target-fights-to-end-bank-suits-a-year-after-data-breach", http://www.bloomberg.com/news/2014-11-21, accessed on 25 Nov 14
