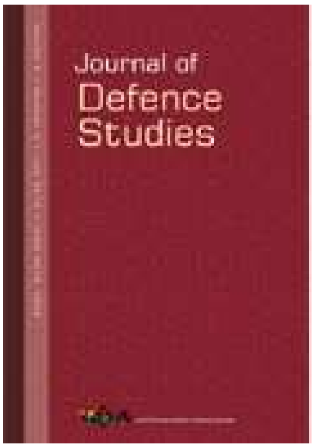

Data Theft: Implications for Economic and National Security

Munish Sharma

Data Theft
Implications for Economic and National Security

Munish Sharma*

With the digitisation of services, such as in the case of governance and banking, or the electronic means of conducting commerce or trade, a large amount of data is generated, stored, processed; this also traverses, over digital devices and networks. The incidents of data theft compromise the integrity of this data. Data is at continuous risk from a myriad of threat actors varying from hacktivists to nation states. When the data is classified or confidential, data breaches and thefts may have grave implications for economic and national security, particularly when nation states and market competitors engage in such practices. The growing number of data theft incidents has emerged as a key cybersecurity challenge for policymakers and security practitioners. The article contemplates the common threat actors and their motivational factors. It analyses data theft instances from the last two years with regard to the implications for economic and national security.

With the burst in online activity for a variety of needs, such as e-commerce, online payments for purchases, utility bills, banking and insurance or securities trade, vast amount of data carrying financial and personal information exchanges hands between the mobile or computer platforms and the respective websites or payment gateways. Data, either personal or financial, is of utmost importance to the owner as well as the malicious actor in pursuit of data. A lot of personal data in the form of e-mail addresses, healthcare records, home addresses, mobile numbers or details of identity cards is stored by these online platforms. In the

* The author is an Associate Fellow (Cyber Security Project) at the Institute for Defence Studies and Analyses (IDSA), New Delhi.

ISSN 0976-1004 print
© 2017 Institute for Defence Studies and Analyses
Journal of Defence Studies, Vol. 11, No. 1, January–March 2017, pp. 61–79

absence of effective security measures, such form of data, much valuable to the individuals whom it belongs to, is at persistent risk.

In the information era, data is an asset. Data is generated or gathered across all the business functions, be it the production, marketing, analytics or strategy aspects of an enterprise. Intellectual property (IP) in form of trade secrets or copyrights underpins both industrial and knowledge economies. Advanced defence technologies assure military superiority; and their research, development and deployment is also a data-intensive exercise. Their designs, blueprints, test data, specifications, configurations, etc., are most sought-after details by military adversaries. The quantum of data thefts is growing every year; and numerous reports have attempted to calculate the quantum of damage to the economies.[1]

A breach of IP, as a much-possessed asset, leads to loss of revenue and opportunity for the victim organisation. The process of developing IP is research and investment intensive. Once compromised, the inventor or the licensees lose their exclusivity over the product or process, which is highly detrimental given the large investments made in the due process of research and development (R&D). Moreover, it undermines the morale of innovators or entrepreneurs as IP thefts take away the incentives. This impedes development of novel ideas and inventions, which basically fuels both the developing and developed economies.[2] If a nation is not able to provide safe and secure cyberspace for entrepreneurs or leading research enterprises, in form of policies, laws or legislations, it faces the risk of losing present as well as future investments. India, as an emerging global R&D hub, has economic development and numerous jobs at risk. Trade secrets are the fundamental building blocks that propel investments, inculcate innovation and boost economic growth. The theft of trade secrets, primarily through cyber means, is emerging as a techno-policy challenge for the management, security professionals and policymakers. It has severe implications for industrial and knowledge-based economies.

By definition, 'Data theft is the illegal transfer or storage of any information that is confidential, personal, or financial in nature, including passwords, software code, or algorithms, proprietary process-oriented information, or technologies.'[3] The loss to the victim may not always be direct and it ranges from reputational damage to the loss of customer trust; financial penalties to the cost of remediation; and could even be in the form of greater competition arising from the stolen information.[4] From an organisational perspective, data theft may amount to any of the following:[5]

1. The loss of IP and business confidential information.
2. The loss of sensitive business information.
3. Opportunity costs, in the form of service or employment disruptions, and customer withdrawal or reduced trust for online activities.
4. The additional cost of securing networks, insurance, regulatory penalties, compensation and recovery from cyber attacks.
5. Reputational damage.

Data thefts can be executed through various vectors, either one of them or a combination of few. Some of the known vectors are:

1. *Universal Serial Bus (USB) drives*: USB ports are provided with every computer system and USB drives are available at such a low cost that their usage has proliferated. They are now considered to be the easiest method of data theft. They are small in size, easy to connect directly with the computer and offer high storage capacity. Using USB drives, if the ports are open, it is quite easy to sneak data out of the premises.
2. *Portable hard drives*: Similar to USB drives, portable hard drives use USB ports and large amount of data can be transferred using them.
3. *Electronic devices/smartphone*: Electronic devices such as music players and sound recorders are also one of the vectors for data theft. These devices have memory storage; and can be connected using Wi-Fi, USB ports or Bluetooth.
4. *Cloud storage and e-mail:* Personal e-mail and cloud storage services such as Yahoo, Gmail, Google Drive and Dropbox allow the users to upload files from their respective devices. These cloud-based applications are accessible easily and are probable vectors for data theft.
5. *Written/printed material:* Data sometimes stored in form of handwritten or printed formats and such material is prone to theft.
6. *Malware/cyber attack:* This category of vector is used when outsiders intrude into the networks of the target, using a malware. Once infected, the malware spreads across the network, looks for the specific set of data or information, communicates with its command and control server and sends the data to the

> designated server across an Internet connection. Malware attacks need a carrier, that is, either the help of an insider or a victim of phishing attack or an infectious USB drive.

Data can exist in many forms, having different valuation and meaning for different organisations. It could be business or financial for an enterprise, or it could be engineering data in form of software programmes, algorithms, designs or prototypes, process flows, blueprints, simulation and testing and performance for an industry. For a bank, it could be the credentials, account information or even the credit/debit card details. For a nation state, information related to its foreign policy, internal security, defence management such as placement or movement of armed forces, information pertaining to research or performance of military hardware (submarines, weaponry, aircrafts, aircraft carriers, frigates), etc., is sensitive in nature, and therefore restricted to a select few. It could be stored physically or through electronic means in computers, servers, graphically or in writing. The plethora of threat actors, foreign intelligence agencies, business competitors, transnational criminal syndicates, hacktivists and insiders, acting in individual capacity or in collusion, pose different degree of economic and national security implications.

Common Threat Actors

The threat actors exploit vulnerabilities to get access to the desired set of data or information. They have their own motivational factors, varying from political to security or monetary gains to rivalry or competition. Similarly, there are a myriad of malicious actors. These could be insiders such as disgruntled employees, adversarial nation states conducting economic or security-related espionage and crime syndicates with transnational presence. All the actors have varying capacities and capabilities to execute data thefts. A nation state, in general, has the wherewithal to conduct massive espionage operations; a crime syndicate can borrow or hire the requisite professional expertise; and insiders have physical access to the systems and networks. Intense competition among enterprises, to gain contracts or control the markets, makes business information an alluring target. Therefore, understanding the threats, their motivations and their means, which is also termed as threat vectors, can help organisations to reduce their exposure to data theft risks.

Nation States

In terms of resources and capabilities, nation states are the most potent threats in the cyber realm. They have extensive expertise as well as financial and computing resources at their disposal to undertake persistent and sophisticated attacks. In order to increase their economic might and gain commanding heights of technology markets and top-of-the-order military hardware, nation states engage in data thefts, although covertly. Even political motivations are a major driver of cyber-led espionage attempts and information thefts.

In 2014, five officers of China's People's Liberation Army (PLA) were indicted by the United States (US) Department of Justice on charges of hacking into the networks of American companies—US Steel, Alcoa, Allegheny Technologies (ATI), Westinghouse, to name a few. The officers were charged with 'Cyber Espionage' against US corporations for commercial advantage, and the victims were mainly from nuclear, metals and solar product industries.[6] Between 2010 and 2012, Westinghouse fell victim to a theft of 1.4 gigabytes of data, roughly 700,000 pages of e-mail and attachments.[7] Similarly, hackers stole the usernames and passwords of at least 7,000 ATI employees while it was in an international trade dispute with a Chinese competitor.[8] Any breach of sensitive information or internal communication is detrimental to the competitive advantage of the victim. The timing of breaches is also important, as these operations are carried out around the bidding of big contracts or negotiations of contracts, litigations or sensitive/high-end product development.

As an emerging threat, a sophisticated, targeted and prolonged attempt of intrusion and information theft is characterised as advanced persistent threat (APT). Such attacks infiltrate into sensitive systems, such as e-mail servers, and remain undetected and hidden from the administrators, sometimes for years. Since APTs are highly advanced and leave hardly any trace, they render forensics incapacitated. These attacks have gained momentum and more instances are being reported, primarily concerning espionage related to cyber, corporate and intelligence operations.

Motivational Factors

Cyber enables asymmetric means of warfare, with a high degree of deniability. For nation states, cyber is a lucrative option, and its usage is generally driven by political/military or economic factors. If it is in the interests of the state to engage in extracting business information and aid the domestic players, it poses a direct threat to business enterprises.

It is often that nation states engage in industrial or corporate espionage. However, the military and advanced technologies are the areas of greater interest to them. Military units or intelligence agencies, backed by the state machinery, are a credible and direct threat to the state. These units are highly specialised and given the availability of resources, both financial and infrastructure, they are used for various purposes, from conducting cyber espionage to crippling the critical infrastructure of the adversary state. The recent instances of personal information theft from the databases of Office of Personnel Management (OPM) of the US and health insurers are being analysed from a nation security perspective, as a foreign hand in these data breaches has been anticipated.

The Insider Threat

The insiders, either present or former employees, are a rich source of information, trade secrets and processed and insider information. Even consultants, legal advisers, auditors or vendors, such as material suppliers or information technology (IT) outsourcing firms, have access to some of the classified information. A disgruntled employee, or for that matter any insider, is a potent and credible threat as he/she has roots deep inside the organisation. Financial gain, revenge or ideological motivation can convince an employee to divulge classified information.[9] The data or information leak could be through written or printed documents, photographs, verbally, sharing of log in credentials, access cards or even through portable media such as USB drives or mobile phones. The latest surveys and studies have been pointing at the emerging trend where major cyber breaches have had an insider hand.

Insider threat has two classifications: (a) malicious insiders; and (b) compromised victims.[10] Phishing or social engineering attacks are targeted at individuals who, by mistake or negligence, click on a link or an e-mail attachment which leads them to compromise the security of their own system or reveal their login or user access credentials. A rigorous cybersecurity awareness or training programme sensitises employees about the precautionary measures related to e-mail communication.

Social engineering techniques are increasingly being used by adversaries to dupe the employees to divulge sensitive information, and often they do so unconsciously. Employees have the necessary access to information, processes and passwords, which are easy gateways for an intruder. Human beings are the weakest link in the information security chain. Once socially engineered or duped using a phishing attempt, an employee can reveal information of the highest order, which otherwise is impossible to gain for an outsider. Mobile devices of the employees, such as laptops and mobile phones, are another emerging set of vectors. These are deemed to be soft targets by threat actors. A stolen mobile phone or laptop can compromise e-mails or text messages, in addition to the information stored on the hard drive.

In May 2013, Edward Snowden, a contractor with the National Security Agency (NSA) of the US, leaked volumes of secret documents to the media, exposing the extensive Internet and phone surveillance activities of intelligence agencies in the US. It revealed the role of nine private players, including Facebook, Google, Microsoft and Yahoo, and the NSA in a massive surveillance programme known as the PRISM. The documents were copied from the NSA without any authorisation. Snowden has been charged in the US with theft of government property and unauthorised communication of national defence information.[11] This is the extent of insider threat: a premiere technical intelligence in the world could not anticipate such a massive data theft. A theft of this scale would definitely not have happened overnight. This incident signifies how potent an insider can be as a threat, and these activities can undergo undetected, despite having state-of-the-art access control systems and checks in place.

Motivational Factors

The most difficult threat to mitigate is the malicious insider(s) threat. It is hard to identify or screen them and equally hard to decipher their underlying motivational factors. They are as diverse as dissatisfaction with the management, poor appraisals, monetary advantage, vengeance, etc. Malicious insiders are well versed with the vulnerabilities of the organisation or its systems, services, products or facilities; they may even implant vulnerabilities intentionally to be exploited later.[12] This set of threat actors—varying from present and former employees to business partners such as contractors, consultants, service providers, vendors and IT integrators—has insider knowledge, which is camouflaged and has a wide scope.

Market/Business Competitors

The markets are globalised today: raw materials are sourced from different countries; and products are designed and engineered across different time zones and then, produced or sold in different markets.

The competition has correspondingly globalised. A Chinese networking or telecom equipment supplier, such as Huawei or ZTE, now competes with Motorola, Nokia Networks, Ericsson and Cisco Systems. Again, in the smartphone market, Huawei, Xiaomi and Lenovo give tough competition to Samsung, Sony and Motorola. Given the strategic nature of energy resources, major Chinese oil and gas companies, Sinopec, China National Petroleum Corporation and PetroChina, are at loggerheads with the likes of Saudi Aramco, ExxonMobil, Royal Dutch Shell and British Petroleum. Amidst the growing competition for control over markets and resources such as strategic materials and energy, competing enterprises conduct espionage, culminating into data thefts.

The US and European oil industry witnessed a massive espionage operation in 2010. The victims found their valuable 'bid data' to be compromised, which had details about the quantity, value and location of oil discoveries worldwide.[13] With the backing of the state, competing enterprises can target sensitive information with the assistance of governmental agencies as well. Therefore, this is not merely competition among the market players but also culminates into economic competition among the nation states.

Motivational Factors

The motivational factor for business competitors is quite direct and clear: to gain advantageous position in the market vis-à-vis the segment competitor. The insider information, such as business or expansion strategy, mergers and acquisitions, contract and bid details, communication among the senior management or board members, and classified trade secrets such as formulations and new product designs or details are all motivational factors for business competitors to engage in cyber enabled or other means of data theft.

Organised Crime Syndicates

Criminal groups have successfully attacked numerous corporate networks to access payment systems and steal personal information such as health records and credit/debit card credentials, which in turn are used to inflict financial damage or extort money. Since these players are technically equipped but outlawed, they are suspected to facilitate other threat actors such as competitors or intelligence agencies, and offer their services to steal trade secrets or personal and business information. They might collude with other actors as well.

Anthem, a major insurance provider in the US, fell victim to a hacking incident in February 2015, when 80 million customer records including details such as names, birthdates, e-mail addresses, Social Security Numbers (SSNs) and medical IDs were compromised.[14] Premera, another insurer, found 11 million records breached, which again had details such as SSNs, financial information and healthcare data related to clinical examination or insurance claims.[15] The attack was led by a phishing e-mail, where compromised employees ended up downloading a Trojan with key logger software that gave the attackers access to unencrypted data through harvested passwords.

The US Securities and Exchange Commission exposed an insider trading practice, an amalgamation of hackers and fraudsters. Hackers gained access to the release data on the servers of distributors such as Business Wire, Market wired and PR Newswire, and investors traded on stocks and made extraordinary profits, equipped with this information, before it went public. The investors traded in the stocks of Boeing, Hewlett-Packard, Caterpillar, Oracle, etc.[16] In 2014, FireEye unveiled an advanced hackers' syndicate, named as FIN4, which targeted the e-mail correspondence of top executives and advisors of large pharmaceutical and financial companies. The group selectively targeted e-mail accounts of the executives, which fetched them business information, and it was further leveraged to trade in stocks.[17]

Motivational Factors

Monetary or financial gains, either through fraudulent activities or leveraging the stolen banking/credit/debit card credentials, are the prime motivational factors. However, these actors are now known to work in collusion with professional hackers and stock market investors, unleashing a whole new segment of criminal offence while booking exorbitant financial gains from securities trade.

Hacktivists

Hacktivists use network or cyber attacks to achieve their political agenda or make their political points. Anonymous, Anon Ghost and the Syrian Electronic Army are few of the known hacktivist groups. Using cyber as a medium to target the political authorities to advance their agenda or express discontentment with some political or policy decisions, hacktivists easily capture the desired media attention by defacing the websites, hacking into social media accounts or executing Distributed

Denial of Service attacks against a high-value target. Hacktivists have the requisite technical knowledge and the desired capabilities to target sensitive information or data, and they become more potent as a threat actor when they collude with other threat actors for ideological or monetary gains.

Motivational Factors

Hacktivists are driven by specific political or social agenda. For them, political activism or pressurising the state to heed to their demands and propagating their ideological stands are the prime objectives as well as motivational factors. But given their growing technological prowess, they are a possible nuisance for the state or political opponents.

Recent Data Thefts: Economic and National Security Implications

In September 2016, Yahoo, the giant online services provider, reported a case of data stolen from its networks, impacting close to half a billion users. Yahoo described it as a 'state-sponsored' attack. This attack is designated as the largest Internet theft on records, and the theft includes names, e-mail addresses, telephone numbers, dates of birth and encrypted passwords.[18] This is not the first case of online services providers falling victim to data thefts. The information of around 427 million users of MySpace was put up for sale on the Dark Web earlier in 2016.[19] LinkedIn, the professional networking website, found information of 117 million accounts put up for sale in May 2016.[20] Similar instances have been witnessed by social blogging website Tumblr[21] and dating site Ashley Madison.[22] These breaches amount to significant financial loss, either through compensation or regulatory liabilities or loss of business. The diminishing trust of users in online activities is not a healthy sign for economic development either. Regarding the security of data, not just the private sector but even the government offices have failed to secure their strategic databases. Annexure 1 summarises major known incidents of data theft in the last two years, according to the quantum of theft, targeted organisation, nature of information or data which was subject to theft and the impact as a result of the breach.

The OPM of the Government of US, in June 2015, discovered that the background investigation records of current, former and prospective federal employees and contractors had been stolen.[23] The investigations revealed that sensitive information, including the SSNs of around 21.5

million citizens, was stolen from the background investigation databases. This was the second discovery of data theft. In the earlier part of 2015, the OPM had discovered that personnel data of 4.2 million current and former federal government employees had been stolen.[24] Data theft, in fact, is not restricted to online identity or accounts of masses; even defence manufacturers have fallen victim to it.

Some similar incidents have also been reported in India. In October 2016, around 3.2 million debit cards were reported to be comprised owing to a malware in the systems of Hitachi Payment Services, a provider of ATMs and point-of-sale services. Some of the major players in the Indian banking market, namely, Axis, HDFC, ICICI and YES, had to block millions of debit cards as a precautionary measure, due to unauthorised transactions on the cards that reportedly originated in China. The incident has been detrimental to building the trust of the users in the safety of banking transactions. Given the government's push towards electronic transactions, security of key services such as banking is vital to the growth of economy around electronic modes of payment. Modern economies rest upon strong banking and financial sectors with swift flow of capital. Even small breaches in core services have a detrimental effect on the growth perspectives of an emerging economy like India.

India, as an epicentre of knowledge economy and a research and production/development hub for IP-driven sectors such as pharmaceuticals and IT, is not immune to data theft. KPMG, in its India's cybercrime survey report of 2015, deducted that Indian pharmaceuticals sector is at risk from cyber-enabled attacks or espionage attempts mainly because it hosts prized IP[25] that is of immense value to criminals, foreign governments and competitors.[26] Indian IT industry, after crossing over 100 billion USD mark, has a significant presence in markets across the globe. The industry is at persistent risk from data theft attempts. Indian defence establishment has also faced numerous data theft attempts and intrusions, targeted at the Defence Research and Development Organisation (DRDO), the Ministry of Defence and the Indo-Tibetan Border Police (ITBP) force.

In August 2016, India's defence project of six Scorpene-class submarines, designed and being built by French shipbuilder DCNS, faced a major data leak to the quantum of over 22,000 pages. The leaked documents detail the entire secret combat capability of the submarines, including sensors, combat management system, torpedo launch system and specifications, communications system and navigation systems.[27] The leak has compromised the information pertaining to:[28]

1. The stealth capabilities of the six new Indian Scorpene submarines.
2. The frequencies at which the submarines gather intelligence.
3. The levels of noise the submarines make at various speeds.
4. Diving depths, range and endurance.
5. Magnetic, electromagnetic and infra-red data.
6. Specifications of the submarine's torpedo launch system and the combat system.
7. Speed and conditions needed for using the periscope.
8. Propeller's noise specifications.
9. Radiated noise levels when the submarine surfaces.

Following the incident, different arguments have been put forth as to whether the data has been leaked from DCNS or Indian Navy. However, there are many possibilities, such as it being a case of oversight where data was not put behind effective controls or a case of hacking. Despite the accusations, it is a clear security threat to the deployment and operations of the submarine fleet under development. Submarines are strategic assets. They are stealth military platforms and underpin the second-strike capability of India's nuclear triad. The detailing of information such as noise levels/specifications and operational frequencies and their range/endurance is sensitive in nature and military adversaries might harness it to their advantage.

Cyber breaches are not uncommon to India. A hack into the sensitive computer systems at the headquarters of the Eastern Naval Command in Visakhapatnam was reported in 2012,[29] where the indigenous nuclear submarine Arihant had been undergoing sea trials. The e-mails of several high-level officials from the Ministry of External Affairs, Ministry of Home Affairs, DRDO and the ITBP were hacked into in 2013.[30]

Defence is a strategically important domain for India, given the geopolitical conditions in the vicinity of India. The theft of data pertaining to the e-mail communication between the officials of the services, R&D plans of defence research establishments such as DRDO and its laboratories or the data related to the design and testing of military platforms, be it aircrafts, submarines or artillery, is strategic in nature. It needs to be secured at any cost, and the requisite processes for the security, during storage or transmission in both India and abroad, are a responsibility of the stakeholders—the owners as well as the vendors and defence contractors.

Conclusion

The incidents of data thefts from the last two years indicate that personal information, such as SSNs and addresses, log-in credentials or passwords are the most sought-after details. These are not the ends in themselves, but the information, traded on the Dark Net quite often, is bought by different actors, and it is further used to either commit financial frauds, extortion or execute social engineering attacks on the employees working in strategically important facilities or organisations. Generally, users are more inclined to use the same password across different online accounts, like social media, e-mail, blogging and sometimes banking. One compromised password could be the key to gain access to a number of different online activities of the user. In the cases of OPM and Yahoo a foreign hand has been suspected and that throws open a plethora of questions and possibilities. Such sensitive information in foreign hands, especially economic/political/military adversaries, is a grave national security threat. The identity theft may reveal a lot about the employees, their addresses, date of birth, their social media activity or even their telephone numbers. Also, most of the governmental databases are electronically connected. Equipped with the desired information or credentials, more information such as healthcare records or history of medical treatment, passport or travel details, meetings or contacts details, and background checks, could be extracted and used for a host of nefarious activities. Cyber breaches and the resulting data theft cases cut across different sovereignties, jurisdictions, laws and rules.

The problem aggregates due to the absence of international cooperative mechanisms for investigation, attribution and prosecution.

Notes

1. Center for Strategic and International Studies, ‘The Economic Impact of Cybercrime and Cyber Espionage’, July 2013, available at http://www.mcafee.com/in/resources/reports/rp-economic-impact-cybercrime.pdf, accessed on 10 September 2016; and Warwick Ashford, ‘Cyber Crime is a Threat to Global Economy’, *Computer Weekly*, 2 February 2015, available at http://www.computerweekly.com/news/2240239300/Cyber-crime-is-a-threat-to-global-economy-says-researcher, accessed on 10 September 2016.

2. The National Bureau of Asian Research, *The Report of the Commission on the Theft of American Intellectual Property*, 2013, available at http://www.ipcommission.org/report/ip_commission_report_052213.pdf, accessed on 10 September 2016.
3. Massachusetts Institute of Technology (MIT), 'What are the Risks to Data', available at https://ist.mit.edu/security/data_risks, accessed on 10 September 2016.
4. Michael Sentonas, 'The Economic Impact of Cybercrime and Cyber Espionage', *Security Solutions Magazine*, 11 March 2014, available at http://www.securitysolutionsmagazine.biz/2014/03/11/the-economic-impact-of-cybercrime-and-cyber-espionage/, accessed on 10 September 2016.
5. Ibid.
6. The US Department of Justice, 'U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage', 19 May 2014, available at https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor, accessed on 14 September 2016.
7. 'USA vs. Wang', United States District Court, Western District of Pennsylvania, 1 May 2014, available at https://archive.org/stream/pdfy-w2j3rR60XuUzoQb5/USA%20v%20Wang%20Complaint,%20Chinese%20Military%20Hackers_djvu.txt, accessed on 14 September 2016.
8. Ibid.
9. Center for Responsible Enterprise and Trade and PricewaterhouseCoopers, 'Economic Impact of Trade Secret Theft', February 2014, available at https://www.pwc.com/us/en/forensic-services/publications/assets/economic-impact.pdf, accessed on 14 September 2016.
10. Nir Polak, 'Looking at Insider Threats from the Outside', *Help Net Security*, 30 July 2014, available at https://www.helpnetsecurity.com/2014/07/30/looking-at-insider-threats-from-the-outside/, accessed on 18 September 2016.
11. 'Edward Snowden: Leaks that Exposed US Spy Programme', *BBC News*, 17 January 2014, available athttp://www.bbc.com/news/world-us-canada-23123964, accessed on 18 September 2016.
12. The US Department of Homeland Security, 'National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat', December 2013, available at https://info.publicintelligence.net/DHS-NRE-InsiderThreats.pdf, accessed on 14 September 2016.
13. Mark Clayton, 'US Oil Industry Hit by Cyberattacks: Was China Involved?', *The Christian Science Monitor*, 25 January 2010, available at http://www.

csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved, accessed on 14 September 2016.

14. Charles Riley, 'Insurance Giant Anthem Hit by Massive Data Breach', *CNN Money*, 6 February 2015, available at http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/, accessed on 20 September 2016.
15. Kate Vinton, 'Premera Blue Cross Breach May Have Exposed 11 Million Customers' Medical And Financial Data', *Forbes*, 17 March 2015, available at http://www.forbes.com/sites/katevinton/2015/03/17/11-million-customers-medical-and-financial-data-may-have-been-exposed-in-premera-blue-cross-breach/#75d159a42143, accessed on 23 December 2016.
16. Ajey Lele and Munish Sharma, 'Hacking + Securities Fraud = New Face of Insider Trading', *IDSA Comment*, 2 September 2015, available at http://www.idsa.in/idsacomments/HackingSecuritiesFraudNewFaceofInsiderTrading_alele_020915, accessed on 20 September 2016.
17. Kristen Dennesen, Jordan Berry, Barry Vengerik and Jonathan Wrolstad, 'FIN4: Stealing Insider Information for an Advantage in Stock Trading?', *FireEye*, 30 November 2014, available at https://www.fireeye.com/blog/threat-research/2014/11/fin4_stealing_insid.html, accessed on 20 September 2016.
18. Maron Dakers, 'Half a Billion Yahoo Users' Data Stolen in "State-sponsored" Hack', *The Telegraph*, 23 September 2016, available at http://www.telegraph.co.uk/business/2016/09/22/half-a-billion-yahoo-users-data-stolen-in-state-sponsored-hack/, accessed on 26 September 2016.
19. Brian Barrett, 'Hack Brief: Your Old Myspace Account Just Came Back to Haunt You', *Wired*, 31 May 2016, available at https://www.wired.com/2016/05/hack-brief-old-myspace-account-just-came-back-haunt/, accessed on 26 September 2016.
20. 'Over 100 Million LinkedIn Profiles Hacked: Here's a Quick Way to Find Out if You're One of Them', *Firstpost*, 29 May 2016, available at http://tech.firstpost.com/news-analysis/over-100-million-linkedin-profiles-hacked-heres-a-quick-way-to-find-out-if-youre-one-of-them-317526.html, accessed on 26 September 2016.
21. Alex Hern, 'More than 65m Tumblr Emails for Sale on the Darknet', *The Guardian*, 31 May 2016, available at https://www.theguardian.com/technology/2016/may/31/tumblr-emails-for-sale-darknet-65-million-hack-passwords, accessed on 26 September 2016.
22. Robert Hackett, 'What to Know about the Ashley Madison Hack', *Fortune*, 26 August 2015, available at http://fortune.com/2015/08/26/ashley-madison-hack/, accessed on 26 September 2016.

23. The US Office of Personnel Management, 'Cybersecurity Resource Center: Cybersecurity Incidents', available at https://www.opm.gov/cybersecurity/cybersecurity-incidents/, accessed on 18 September 2016.
24. Ibid.
25. In the context of the pharma, the IPs targeted include: drug discovery programmes, clinical development programmes, drug registration applications, molecular formulae, patient records, production processes, manufacturing records, quality assurance and compliance data.
26. Utkarsh Palnitkar, 'Rising Spectre of Cybercrime in the Pharmaceutical Sector', *The Economic Times*, 13 February 2016, available at http://articles.economictimes.indiatimes.com/2016-02-13/news/70592990_1_pharma-sector-cybercrime-pharma-companies, accessed on 21 September 2016.
27. Cameron Stewart, 'Our French Submarine Builder in Massive Leak Scandal', *The Australian*, 29 August 2016, available at http://www.theaustralian.com.au/national-affairs/defence/our-french-submarine-builder-in-massive-leak-scandal/news-story/3fe0d25b7733873c44aaa0a4d42db39e,accessed on 18 September 2016; and 'Secret Data on India's Scorpene Submarine Leaked: Report', *The Indian Express*, 26 August 2016, available at http://indianexpress.com/article/india/india-news-india/scorpene-submarine-leak-sensitive-data-indian-navy-france-dcns/, accessed on 18 September 2016.
28. Ibid.
29. P.K. Vasudeva, 'Secure Our e-frontiers', *Hindustan Times*, 12 July 2012, available at http://www.hindustantimes.com/india/secure-our-e-frontiers/story-orh6I0tb5ZUyMbheH5PJDM.html, accessed on 9December 2016.
30. Manu Kaushik and Pierre Mario Fitter, 'Beware of the Bugs', *Business Today*, 17 February 2013, available at http://www.businesstoday.in/magazine/features/india-cyber-security-at-risk/story/191786.html, accessed on 9 December 2016.

Annexure 1 Major Data Thefts/Breaches in the Last Two Years

Targeted Organisation	*Industry/ Vertical*	*Quantum of Theft*	*Details of Theft Data/ Information*	*Origin/Impact*
eBay (2014)	e-commerce	145million users	• Names; • addresses; • e-mail addresses; • encrypted passwords; and • dates of birth.	• Perpetrated by stealing employee credentials. • Direct loss of business for eBay due to breach of trust.
Sony (2014)	Entertainment	47,000 employees and actors	• Personal information of employees. • Personal information of actors. • Leak of movies in production.	• A hacker group called 'Guardians of Peace' claimed responsibility. • Sony's stock price dropped. • Copyright infringement and legal issues.
Ashley Madison (2015)	Online services	37 million users	• Sensitive customer details posted on the Dark Web.	• A hacker group called 'The Impact Team' claimed responsibility. • Breach of customer trust/reputation loss.
Talk Talk (2015)	Phone and broadband provider	157,000 customers	• Bank account numbers; • sort codes; and • credit card details.	• Three call centre employees breached policies and the terms of contract. • Potential loss of business for the contractor/vendor. • Cost the company £60 million. • Lost 95,000 customers.

Targeted Organisation	*Industry/ Vertical*	*Quantum of Theft*	*Details of Theft Data/ Information*	*Origin/Impact*
Office of Personnel Management (OPM) (2015)	Government	21.5 million former and prospective federal employees	• Background investigation records; • biometric details; and • SSNs.	• Risk of exploitation by foreign entities. • Potential risk for sensitive national security data: electronic linkages between the OPM security clearance files, Department of Defense service records and State Department passport records. • Exposed former and serving Federal employees to social engineering risks.
Anthem (2015)	Healthcare (insurance)	80 million customer records	• Names; • Birthdates; • e-mail addresses; • SSNs; and • medical IDs.	• Use harvested data to launch social engineering attacks or blackmail. • Trick worried consumers into sharing confidential information such as financial details.
Premera (2015)	Healthcare (insurance)	11 million customer records	• SSNs; • financial information; and • healthcare data of clinical and insurance claims.	• Use harvested data to launch social engineering attacks or blackmail. • Trick worried consumers into sharing confidential information such as financial details. • Selling off the data on Dark Web.
LinkedIn (2016)	Online services (professional networking)	117 million users	• Account details.	• Customer credentials sold on Dark Web marketplace, ‘The Real Deal’. • Breach of customer trust and loss of reputation. • Compensation to premium account holders. • Risk for customers using same passwords across multiple online accounts.

Targeted Organisation	*Industry/ Vertical*	*Quantum of Theft*	*Details of Theft Data/ Information*	*Origin/Impact*
MySpace (2016)	Social media	427 million users	• Passwords; and • e-mail addresses.	• Risk for customers using same passwords across multiple online accounts.
DCNS (Scorpene-class Submarines) (2016)	Defence manufacturing	22,000 pages	• Secret combat capability of the submarines. • Sensors information. • Combat management system. • Torpedo launch system and specifications. • Communications and navigation systems.	• Compromised sensitive performance information—direct national security risk. • Potential risk to other customers of DCNS, that is, Australia and Brazil. • Thales(35 per cent shareholder) shares fell by 3 percent. • Potential impact on future projects.
Yahoo (2016)	Online services	500 million users	• Names; • e-mail addresses; • telephone numbers; • dates of birth; and • encrypted passwords.	• Risk to $4.8billion sale of Yahoo's core business to Verizon. • Users at risk from phishing/social engineering attacks. • Potential risk from loss of business/ customer withdrawal.
Multiple banks—Axis, HDFC, ICICI, YES (2016)	Banking	3.2 million debit cards	• Debit card details. • Unauthorised transactions. • ATMs compromised.	• Unauthorised transactions reportedly originated in China. • Caused by a malware in the systems of Hitachi Payment Services, a provider of ATMs and point-of-sale services. • Millions of debit cards blocked as precautionary measure.

Source: Compiled by author, sourced from different news websites.