2015

Guneet Kaur Pahwa

3rd year student of B.Tech (IT)
Maharaja Agrasen Institute of Technology
GGSIPU

[CYBER BUSINESS SECURITY THREATS & SOLUTIONS]

Submitted to
CMAI Association of India

Under the guidance of
Prof. NK Goyal

INDEX

ACKNOWLEDGEMENT

"It is impossible to prepare a project report without the assistance & encouragement of other people. This one is certainly no exception."

On the very outset of this report, I would like to extend my sincere & heartfelt obligation towards all the personages who have helped me in this endeavor. Without their active guidance, help, cooperation & encouragement, I would not have made headway in the project.

I am ineffably indebted to Prof. NK Goyal for conscientious guidance and encouragement to accomplish this assignment.

I extend my gratitude to Maharaja Agrasen Institute of Technology for giving me this opportunity. I also acknowledge with a deep sense of reverence, my gratitude towards my parents and member of my family, who has always supported me morally as well as economically.

Any omission in this brief acknowledgement does not mean lack of gratitude.

INTRODUCTION

CYBER INSECURITY a major threat to businesses today:
Along with the world, which continues to embrace the ever evolving technology and its advantages, businesses have also started relying on technology extensively for storing great amount of sensitive data electronically. The ease in storing and accessing information has led to its increasing popularity. Along with the efficiencies the computer brings to the life of many, it has inadvertently created a new area of risk. The storage of sensitive information on computers opens business up to cyber-attacks, with hackers looking to acquire company or customer information such as passwords or credit card numbers. The hackers can then use or sell this information, harming businesses, consumers, and company reputations.

Many high profile security breaches have highlighted the issue of Cyber-Attacks. These attacks have left companies struggling to improvise on these issues, but what becomes an even major problem is regaining the trust of the customers and reassuring them that their sites and accounts are safe from any further attacks.

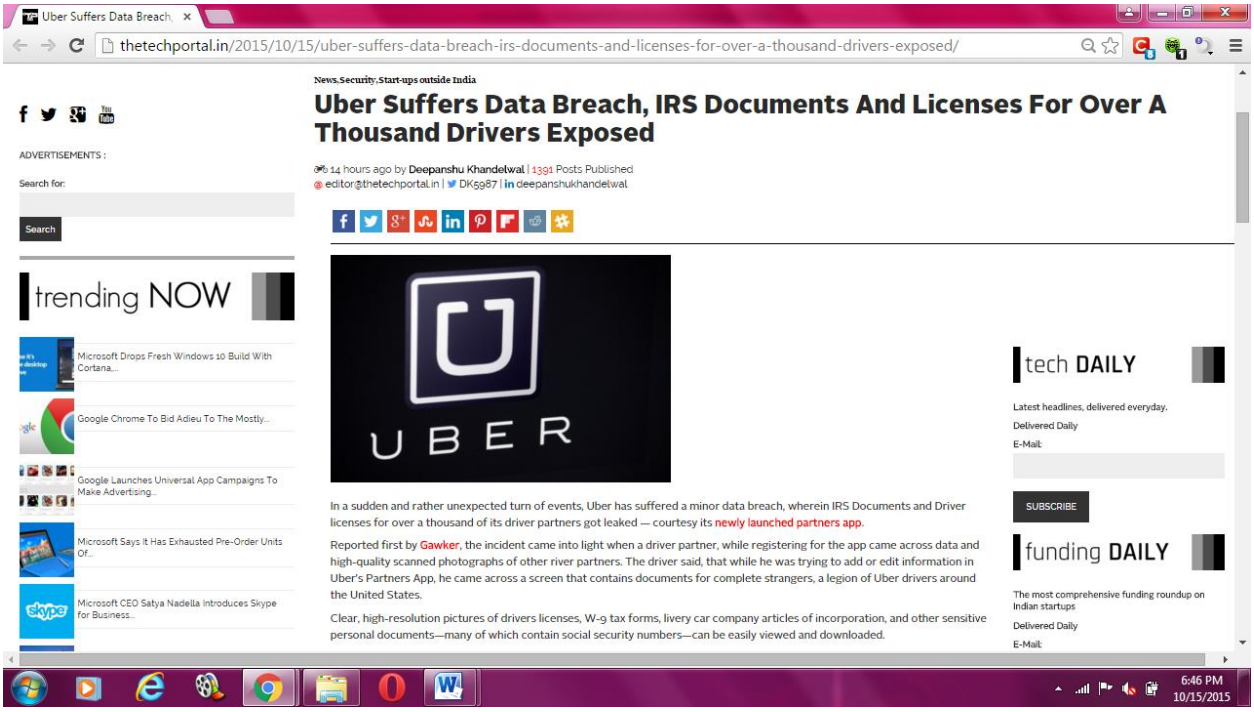
In a survey conducted in India by KPMG, which consisted of 170 CIOs (Chief Information Officers) and CISOs (Chief Information Security Officers), it was found out that, with rise in the cybercrime, businesses are increasingly facing impacts not only on the financial front but also irreversible damage to their brands and market reputations. 89% respondents agreed that Cybercrime has emerged as a major threat, 51% claimed to be an "easy target". Further it revealed that over the years, the target of the cyber-attacks has shifted from theft of financial information to business espionage and government information.

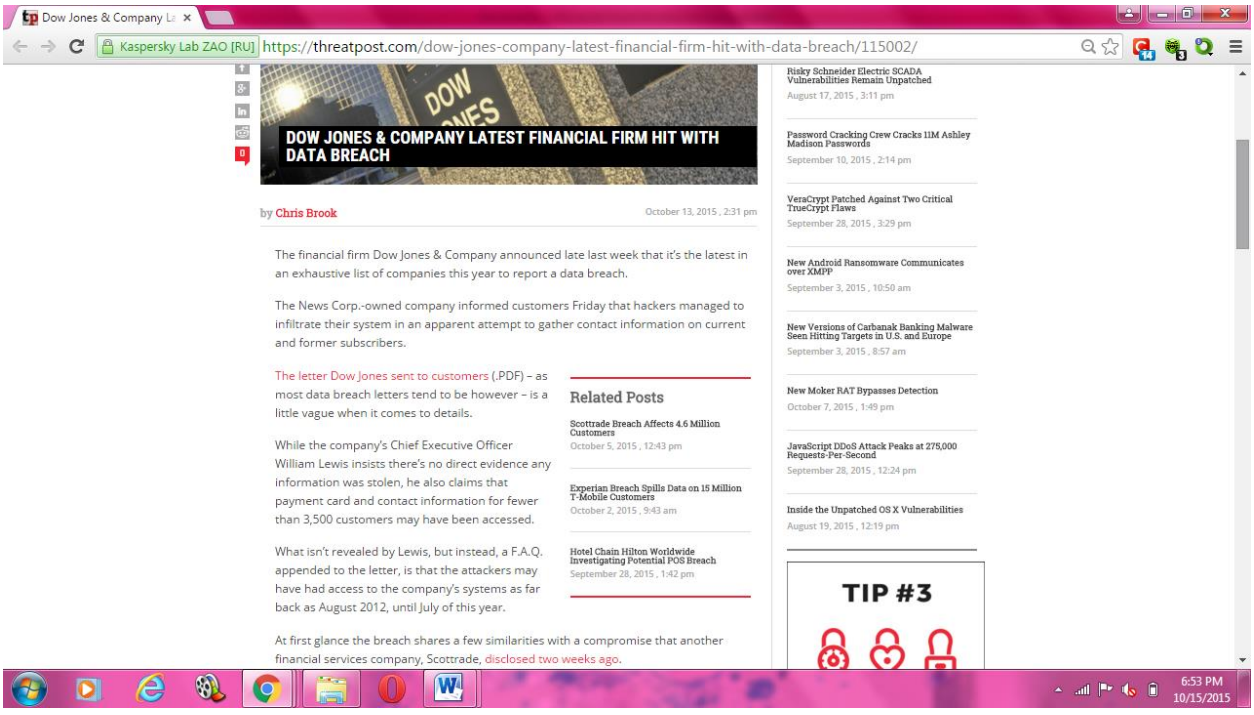
Being a developing country, and due to many other factors, even today India is not 100% digitalized and a lot of work is still done manually. Even after this, according to India Risk Survey 2014 report, Information and Cyber Insecurity is among the top 3 risks in India in industrial sectors like IT/ITES and Financial Services, and ranks 5th when it comes to the majors risks the country is facing today.

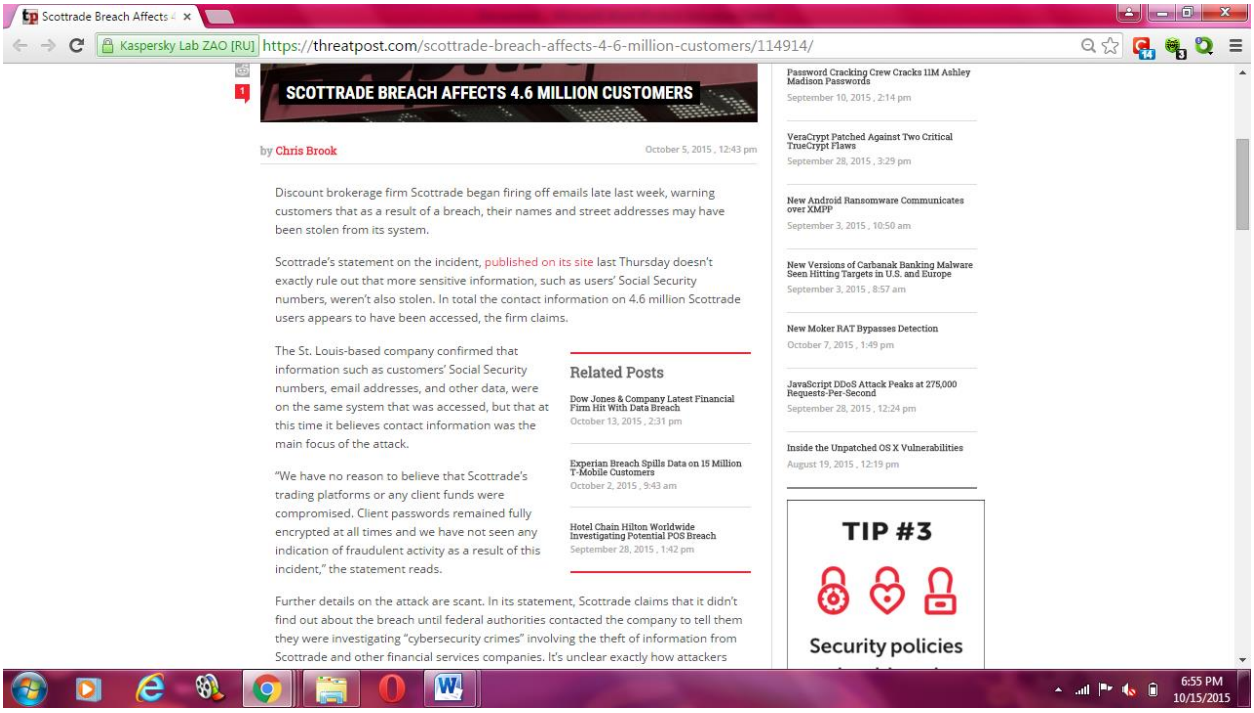
As businesses look at the costs associated with cyber-attacks, insurance for these security breaches is becoming more popular. In 2012, over $1.3 billion was spent on cyber insurance premiums, and the number grew by manifolds in 2014. The problem for businesses is that as of now, cyber-insurance will only cover up to $300 million at most for breaches, which can be much less than the financial damages surrounding the loss in reputation for major corporations. As businesses continue to adapt to the ever changing technological world, more investment will be needed in improvements in security and technological innovation to counter attacks prior to the breaches occurring. Until these advances occur, more companies will be forced to buy cyber-insurance, and these new costs will eventually be passed to the consumer.

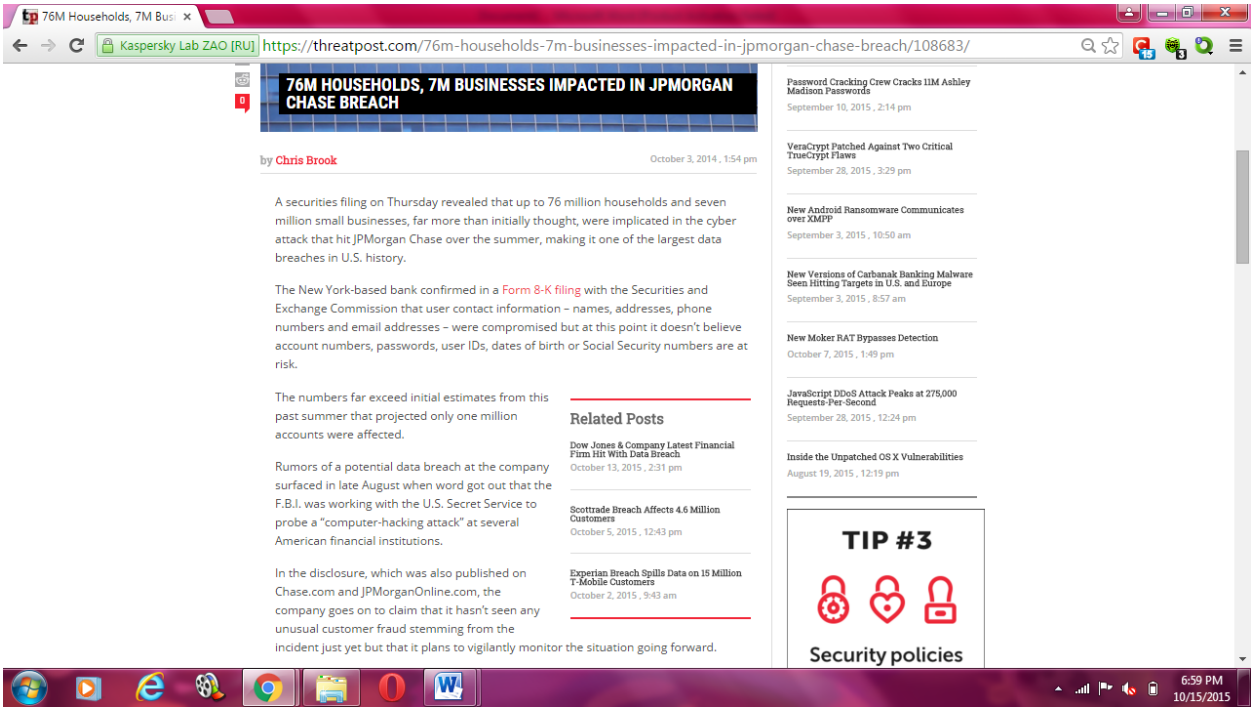
Cyber-crime today, has become a business, and the hackers are looking for real dollars, & this business is expanding day by day. Various businesses, big or small fall into this trap every day.

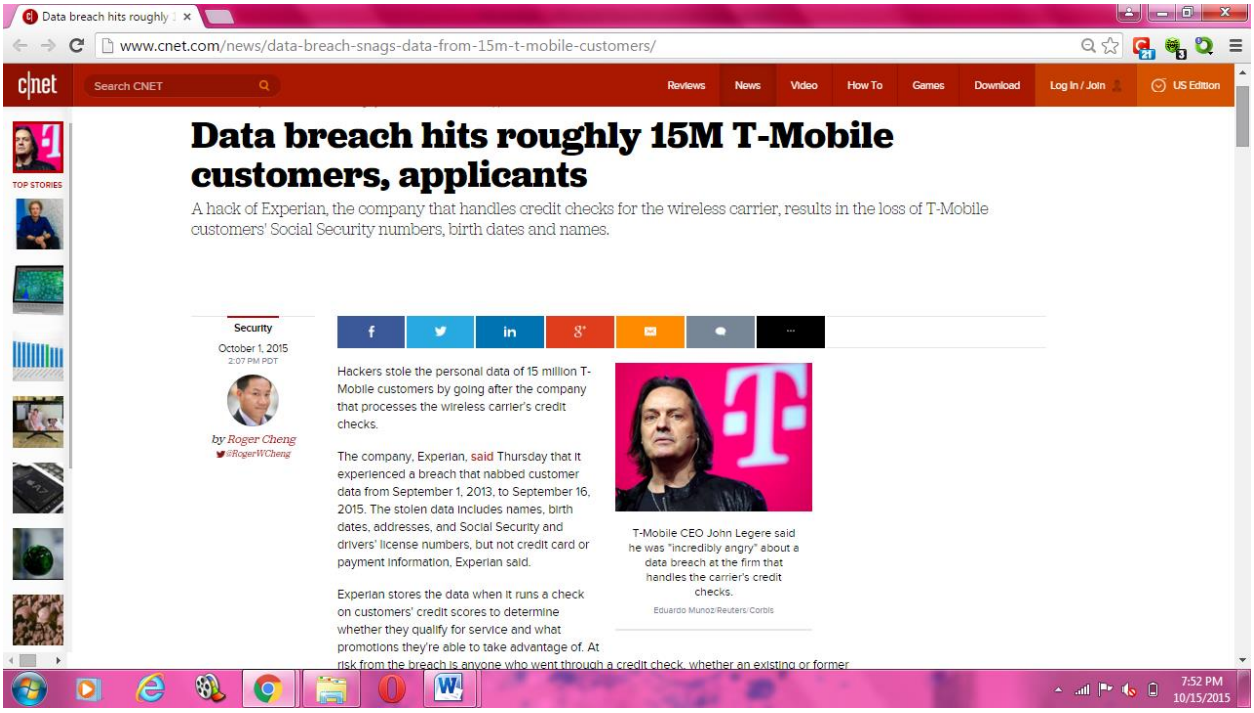
THE NEED FOR CYBER SECURITY IS REAL

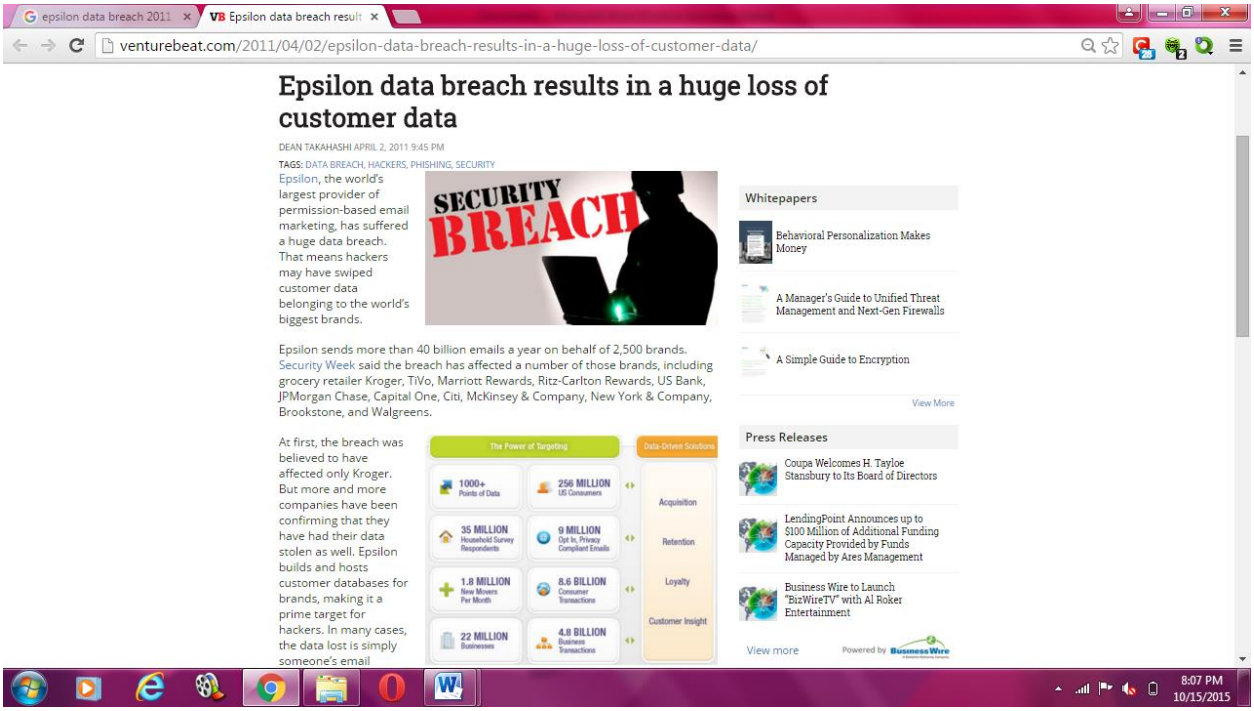





Scottrade Breach Affects
Kaspersky Lab ZAO [RU] https://threatpost.com/scottrade-breach-affects-4-6-million-customers/114914/
SCOTTRADE BREACH AFFECTS 4.6 MILLION CUSTOMERS
by Chris Brook
October 5, 2015 , 12:43 pm
Discount brokerage firm Scottrade began firing off emails late last week, warning customers that as a result of a breach, their names and street addresses may have been stolen from its system.
Scottrade's statement on the incident, published on its site last Thursday doesn't exactly rule out that more sensitive information, such as users' Social Security numbers, weren't also stolen. In total the contact information on 4.6 million Scottrade users appears to have been accessed, the firm claims.
The St. Louis-based company confirmed that information such as customers' Social Security numbers, email addresses, and other data, were on the same system that was accessed, but that at this time it believes contact information was the main focus of the attack.
"We have no reason to believe that Scottrade's trading platforms or any client funds were compromised. Client passwords remained fully encrypted at all times and we have not seen any indication of fraudulent activity as a result of this incident," the statement reads.
Related Posts
Dow Jones & Company Latest Financial Firm Hit With Data Breach
October 13, 2015 , 2:31 pm
Experian Breach Spills Data on 15 Million T-Mobile Customers
October 2, 2015 , 9:43 am
Hotel Chain Hilton Worldwide Investigating Potential POS Breach
September 28, 2015 , 1:42 pm
Further details on the attack are scant. In its statement, Scottrade claims that it didn't find out about the breach until federal authorities contacted the company to tell them they were investigating "cybersecurity crimes" involving the theft of information from Scottrade and other financial services companies. It's unclear exactly how attackers
Password Cracking Crew Cracks 11M Ashley Madison Passwords
September 10, 2015 , 2:14 pm
VeraCrypt Patched Against Two Critical TrueCrypt Flaws
September 28, 2015 , 3:29 pm
New Android Ransomware Communicates over XMPP
September 3, 2015 , 10:50 am
New Versions of Carbanak Banking Malware Seen Hitting Targets in U.S. and Europe
September 3, 2015 , 8:57 am
New Moker RAT Bypasses Detection
October 7, 2015 , 1:49 pm
JavaScript DDoS Attack Peaks at 275,000 Requests-Per-Second
September 28, 2015 , 12:24 pm
Inside the Unpatched OS X Vulnerabilities
August 19, 2015 , 12:19 pm
TIP #3
Security policies
6:55 PM
10/15/2015


76M Households, 7M Bus
Kaspersky Lab ZAO [RU] https://threatpost.com/76m-households-7m-businesses-impacted-in-jpmorgan-chase-breach/108683/
76M HOUSEHOLDS, 7M BUSINESSES IMPACTED IN JPMORGAN CHASE BREACH
by Chris Brook
October 3, 2014 , 1:54 pm
A securities filing on Thursday revealed that up to 76 million households and seven million small businesses, far more than initially thought, were implicated in the cyber attack that hit JPMorgan Chase over the summer, making it one of the largest data breaches in U.S. history.
The New York-based bank confirmed in a Form 8-K filing with the Securities and Exchange Commission that user contact information – names, addresses, phone numbers and email addresses – were compromised but at this point it doesn't believe account numbers, passwords, user IDs, dates of birth or Social Security numbers are at risk.
The numbers far exceed initial estimates from this past summer that projected only one million accounts were affected.
Rumors of a potential data breach at the company surfaced in late August when word got out that the F.B.I. was working with the U.S. Secret Service to probe a "computer-hacking attack" at several American financial institutions.
In the disclosure, which was also published on Chase.com and JPMorganOnline.com, the company goes on to claim that it hasn't seen any unusual customer fraud stemming from the incident just yet but that it plans to vigilantly monitor the situation going forward.
Related Posts
Dow Jones & Company Latest Financial Firm Hit With Data Breach
October 13, 2015 , 2:31 pm
Scottrade Breach Affects 4.6 Million Customers
October 5, 2015 , 12:43 pm
Experian Breach Spills Data on 15 Million T-Mobile Customers
October 2, 2015 , 9:43 am
Password Cracking Crew Cracks 11M Ashley Madison Passwords
September 10, 2015 , 2:14 pm
VeraCrypt Patched Against Two Critical TrueCrypt Flaws
September 28, 2015 , 3:29 pm
New Android Ransomware Communicates over XMPP
September 3, 2015 , 10:50 am
New Versions of Carbanak Banking Malware Seen Hitting Targets in U.S. and Europe
September 3, 2015 , 8:57 am
New Moker RAT Bypasses Detection
October 7, 2015 , 1:49 pm
JavaScript DDoS Attack Peaks at 275,000 Requests-Per-Second
September 28, 2015 , 12:24 pm
Inside the Unpatched OS X Vulnerabilities
August 19, 2015 , 12:19 pm
TIP #3
Security policies
6:59 PM
10/15/2015


Data breach hits roughly
www.cnet.com/news/data-breach-snags-data-from-15m-t-mobile-customers/
cnet
Search CNET
Reviews
News
Video
How To
Games
Download
Log In / Join
US Edition
TOP STORIES
Data breach hits roughly 15M T-Mobile customers, applicants
A hack of Experian, the company that handles credit checks for the wireless carrier, results in the loss of T-Mobile customers' Social Security numbers, birth dates and names.
Security
October 1, 2015
2:07 PM PDT
by Roger Cheng
@RogerWCheng
Hackers stole the personal data of 15 million T-Mobile customers by going after the company that processes the wireless carrier's credit checks.
The company, Experian, said Thursday that it experienced a breach that nabbed customer data from September 1, 2013, to September 16, 2015. The stolen data includes names, birth dates, addresses, and Social Security and drivers' license numbers, but not credit card or payment information, Experian said.
Experian stores the data when it runs a check on customers' credit scores to determine whether they qualify for service and what promotions they're able to take advantage of. At
T-Mobile CEO John Legere said he was "incredibly angry" about a data breach at the firm that handles the carrier's credit checks.
Eduardo Munoz/Reuters/Corbis
7:52 PM
10/15/2015


epsilon data breach 2011
Epsilon data breach result
venturebeat.com/2011/04/02/epsilon-data-breach-results-in-a-huge-loss-of-customer-data/
Epsilon data breach results in a huge loss of customer data
DEAN TAKAHASHI APRIL 2, 2011 9:45 PM
TAGS: DATA BREACH, HACKERS, PHISHING, SECURITY
Epsilon, the world's largest provider of permission-based email marketing, has suffered a huge data breach. That means hackers may have swiped customer data belonging to the world's biggest brands.
SECURITY BREACH
Epsilon sends more than 40 billion emails a year on behalf of 2,500 brands. Security Week said the breach has affected a number of those brands, including grocery retailer Kroger, TiVo, Marriott Rewards, Ritz-Carlton Rewards, US Bank, JPMorgan Chase, Capital One, Citi, McKinsey & Company, New York & Company, Brookstone, and Walgreens.
At first, the breach was believed to have affected only Kroger. But more and more companies have been confirming that they have had their data stolen as well. Epsilon builds and hosts customer databases for brands, making it a prime target for hackers. In many cases, the data lost is simply someone's email
The Power of Targeting
Data-Driven Solutions
1000+ Points of Data
256 MILLION US Consumers
35 MILLION Household Survey Respondents
9 MILLION Opt In, Privacy Compliant Emails
1.8 MILLION New Movers Per Month
8.6 BILLION Consumer Transactions
22 MILLION Businesses
4.8 BILLION Business Transactions
Acquisition
Retention
Loyalty
Customer Insight
Whitepapers
Behavioral Personalization Makes Money
A Manager's Guide to Unified Threat Management and Next-Gen Firewalls
A Simple Guide to Encryption
View More
Press Releases
Coupa Welcomes H. Tayloe Stansbury to Its Board of Directors
LendingPoint Announces up to $100 Million of Additional Funding Capacity Provided by Funds Managed by Ares Management
Business Wire to Launch "BizWireTV" with Al Roker Entertainment
View more
Powered by BusinessWire
8:07 PM
10/15/2015


Third Hacking Team Flash
krebsonsecurity.com/2015/07/third-hacking-team-flash-zero-day-found/
LogRhythm
The Security Intelligence Company
START NOW
Follow me on Twitter
Join me on Facebook
KrebsonSecurity
In-depth security news and investigation
BLOG ADVERTISING
ABOUT THE AUTHOR
13 Third Hacking Team Flash Zero-Day Found
JUL 15
For the third time in a week, researchers have discovered a zero-day vulnerability in Adobe's Flash Player browser plugin. Like the previous two discoveries, this one came to light only after hackers dumped online huge troves of documents stolen from Hacking Team — an Italian security firm that sells software exploits to governments around the world.
News of the latest Flash flaw comes from Trend Micro, which said it reported the bug (CVE-2015-5123) to Adobe's Security Team. Adobe confirmed that it is working on a patch for the two outstanding zero-day vulnerabilities exposed in the Hacking Team breach.
We are likely to continue to see additional Flash zero day bugs surface as a result of this breach. Instead of waiting for Adobe to fix yet another flaw in Flash, please consider removing or at least hobbling this program.
Advertisement
ALIEN VAULT
2015 REPORT:
SANS Cyber Threat Intelligence Survey
DOWNLOAD THE REPORT
8:14 PM
10/15/2015

HACKING

According to the Practical Law Company, Whitepaper on Cyber Attacks, the definition of Cyber Attacks is as follows:

A Cyber Attack is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it.

The definition has 3 distinct factors:

1) Attack or an illegal attempt to
2) Gain something from a
3) Computer system

Generally speaking, a system is a collection of units that work collectively towards a common goal. Thus, whether it is a single or a collection of computers – offline or online (websites/intranets), it is a system as they work to facilitate something or the other. Even a single computer has many components that work together for a common goal and hence is called a computer system.

The main factor is illegal access to such a system. The second factor is target system. The final factor is gains to the attacker. It should be noted that, illegal access must have a motive to compromise the target system, in a way that the attacker gains something, such as information stored in the system, or the total control of system.

REASONS TO HACK

Main reasons behind Hacking may be:

1. To use your computer:
As an Internet Relay Chat (IRC) server – hackers wouldn't want to discuss openly about their activities on their 'own' servers as Storage for Illicit Material (ex. pirated software, pirated music, pornography, hacking tools etc.) as part of a DDoS Attack – where many computers are controlled by hackers in an attempt to cause resource starvation on a victim's computers or networks.

2. To steal services and/or valuable files

3. For thrill and excitement

4. To get even – maybe an IT staff who was terminated, or other parties you've 'wronged'

5. As a publicity stunt – an example of which was reported in 1998 by Jim Hu in MTV "hack" backfires

6. Knowledge/Experiment/Ethical – some hackers probe a computer system to find its security vulnerabilities and then inform the system administrator to help improve their security

7. Another possible reason is that the hackers might suffer from a disease called Asperger syndrome (AS). They are people who are very good with numbers and at focusing on a problem for a very long period of time, but are not good in social relationships. How AS can possibly be linked to hacking behavior was discussed

more thoroughly by M.J. Zuckerman in his 'USA Today' article, What fuels the mind of a hacker?

8. Curiosity

9. To spy on friends, family members or even business rivals

10. Prestige – bragging rights in their social circle (particularly if they've hacked high-profile sites or systems)

11. Intellectual Challenge

12. Money – although most hackers are not motivated by financial gain; many professional criminals make money by using hacking techniques either to set up fake e-commerce sites to collect credit card details gain entry to servers that contain credit cards details engage in other forms of credit card fraud

DATA BREACH

A data breach is an incident in which an unauthorized Hacker or Attacker potentially views, steals or uses sensitive, protected or confidential data from a secure database or repository. It is a type of security breach specifically designed to steal logical or digital data, (often conducted over the Internet or a network connection) and/or publish data to an unsecured or illegal location. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

The most common concept of a data breach is an attacker hacking into a corporate network to steal sensitive data. A hacker also may use stolen data to impersonate himself to gain access to a more secure location.

REASONS OF DATA BREACHES

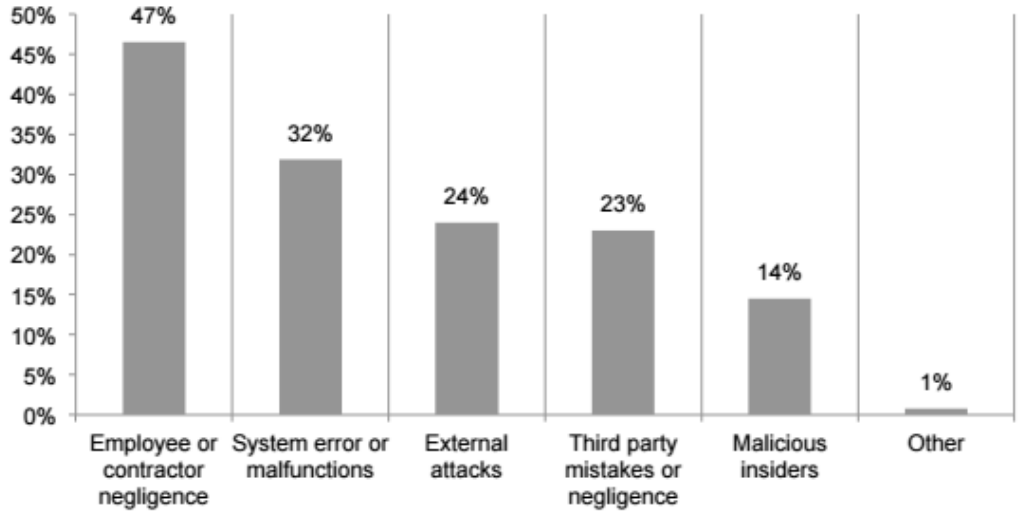
Reasons for Data Breaches can be classified into two:

a) Non-Malicious

b) Malicious

1. Insiders
2. Outsiders

Data breaches have become a fact of life for organizations of all sizes, in every industry and in many parts of the globe. While many organizations anticipate that at some point a non-malicious or malicious data breach will occur, the focus of this study is to understand the steps organizations are taking to deal with the aftermath of a breach or what we call the Post Breach Boom.



Non-Malicious (Due to Ignorance)

1. Simple passwords

Applying passwords at various steps to access the data is not sufficient to safeguard the data today. Keeping default passwords or easy passwords result in creating a threat to the data. Many people realize that to avoid hacking, strong passwords are a must, but they fail to understand that the hackers/crackers are becoming sophisticated day by day.

Through social engineering or by guessing the passwords, they can easily break into the systems. One should therefore keep changing the passwords frequently and should be up to date with the latest techniques in use.

Methods to crack passwords:

a) Guessing-

Various programs have been developed to guess a person's password, with any sort of personal information gained regarding him, from names, DOB, pet's name, license number etc. These programs are capable of searching a word spelled backwards. That is why it is advised to clear any personal information from one's password.

b) Dictionary based attacks-

Certain programs have been developed, which run each and every word of the dictionary against a username in hope of finding a perfect match. Therefore it is advised to keep away from dictionary words of even the remotest language.

c) Brute-Force attack-

By trying every conceivable combination of the keystrokes against a user name, Brute-Force attack is the most successful attack, and many programs

can run this attack very quickly. Therefore it is advised to use a combination of upper and lower case words along with numbers and special characters and punctuation marks.

d) Phishing–

Phishing scams are aimed to trick the person through IM or e-mails to provide their personal information. They might excite the recipient to respond. The best way to avoid being fooled is to not click on any such suspicious links.

e) Shoulder surfing

Passwords are not always stolen online. The hacker may be standing behind you peeping in when you type your password. One should be careful and develop a habit of typing the password fast and by not looking at the keyboard.

Cyber security is based on the "weakest link", and usually the password becomes that part of the chain which can be easily broken. Hence to create and maintain a strong password is very necessary.

While creating a password, a few points should be kept in the mind:

i. Passwords are case sensitive, so a mixture of upper and lower case letters should be used
ii. The password should contain numerals & special characters randomly to make it strong.
iii. Password should be long and complex but sensible enough for you to remember.
iv. The password should be made to type quickly so that anyone looking over cannot catch it.

2. Allowing unrestricted access to all employees

When unrestricted access is given the employees, they can misuse the freedom given to them. Company data and property is at their exposure. In such cases, not only they can sell the company data outside for financial gains but also abrupt the company server, by infecting the systems or exposing the company network to any outsider (knowingly or unknowingly). Therefore it is very important that the employees have restrictions as to what data they can access, what sites they can visit on the internet, what BYODs they can bring to the office or use on the company network.

Many employees have the mentality that because they can access the internet free of cost and a good speed (cost is on the company) in the office, they download & upload data (movies, songs, pictures etc.). They tend to forget that they might infect the system by the various malwares that are waiting on the internet to infect the computers creating their own network. The compromised computer may infect the others on the company network, hence causing a big loss to the company and company data. Many people may use the company owned computers for illegal activities like pornography or to harass coworkers or gamble etc. this can be avoided if they are given limited internet access. Also, unrestricted access to internet may allow the users to socialize the entire time they are in office, not only affecting their performance but also company reputation. Therefore restrictions on web surfing is important in companies.

Moreover the employees should not be allowed to carry pen drives or CDs of any kind. The systems should have facilities of being incompatible to external storage. The main reason behind this is that, the worker will not be able to carry company information outside the office for any purpose. Also, with this the risk of malwares that might be brought to the company network through these devices is avoided.

3. Unpatched vulnerabilities

After the release of any software, as and when it comes to use, the drawbacks and vulnerabilities come into light. The various ways in which they can be exploited for malicious activities are recognized, and the company releases the patches. If these patches are not updated, they can leave the software vulnerable to attacks, thus putting the security of the network at a risk. Therefore it is recommended that companies keep their software up to date, so that this sort of a problem does not arise. In fact according to HP's 2015 Cyber Risk Report, 44% of the breaches in 2014 were dues to the vulnerabilities which were 2-4 years old, and their patches had been released.

4. Sensitive data kept unencrypted

No matter how much care is taken, a hackers' mind is unpredictable. He can by any means reach your data if he intends to and access all he wanted to in the first place, and all the efforts can go waste. But, then the company can prove that, it is smarter. If the sensitive data of the company is kept encrypted, even after reaching the data, the hacker will not be able to recover it.

Encryption is the most effective method for data security. It is technique by which the important messages and data are encoded, so that only authorized users can have access to them because they cannot be decoded without the key. In cryptography, the message or the information which is called the plaintext is encrypted using, what is called encryption algorithm, generating cipher text that can be read on if decrypted. Encryption can be used to protect data "at rest", such as files on computers and storage devices (e.g. USB flash drives).

In recent years there have been numerous reports of confidential data such as customers' personal records being exposed through loss or theft of laptops or backup drives. Encrypting such files at rest helps protect them should physical security measures fail.

Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years. Data should also be encrypted when transmitted across networks

in order to protect against eavesdropping of network traffic by unauthorized users.

Today various encryption algorithms have been developed, some of them which cannot be decrypted without the key. The company can also use a combination of algorithms making the decryption even more difficult. There are three types of encryptions, hashing function, symmetric method (aka private key) and asymmetric method (aka public key).
Various famous encryption techniques in use today are,

- CAST-128
- AES (Rijndael)
- Blowfish
- GOST 28147-89
- RC 6
- Serpent
- Twofish

5. Assuming everything is alright and avoiding regular audits

A common mistake companies may make is, not regularly monitor their security system. Having a security system in place is important but maintaining it and regularly monitoring it, is equally important. Many breaches do not happen overnight. They are result of hackers placing files and collecting information from the server over time. Therefore regular monitoring and review of any discovered discrepancies is very important. Data fraud is a billion dollar business for the hackers, but companies being a little aware can avoid being victimized by this online version of a war.

MALICIOUS

INSIDERS
(Disgruntled Employees)

A disgruntled employee in a company may arise due to the following factors, which as a leader an employer lacks must have:

1. Inspire and Motivate –he is not able to energize his employees for an exceptional result.
2. Trust – over the time he must have lost the trust of the employees.
3. Develops Others – he just wants his targets to be accomplished, and is not bothered about the development of his employees
4. Communicates Powerfully – lacks the ability to provide definite sense of direction and purpose.
5. Integrity and Honesty – shoves his responsibilities off to someone else's shoulders and is never true to his own words
6. Relationship Building – is not able to balance getting results with the concerns for others.
7. Provide secure environment- according to a research by the University of British Columbia, disgruntled employees are a result of bullying at workplace.

These signs can give rise to three types of employees:

1. Unhappy Employees
2. Unethical Employees
3. Fired Employees

All these people have access to the company network, and so can cause a great damage. They use their access to company network to destroy data, obtain customer information, or gain a competitive edge at a new company. They can also sell the data to rival companies for their financial benefits harming the

former's reputation and eventually causing the breakdown of the company. There have been many incidents where disgruntled or former employees have tried to exploit the employer by putting a checkhold on the company website, modifying and restricted access.

The CIO and his team should be able to track all the sensitive information. They should be aware of who is accessing their information, at what location and on what device. This will help to keep a track of unwanted access. If the remote device gets compromised, they should remotely lock it down, wipe it or initiate a self-destruct sequence to remove all the data to protect themselves from stakeholders. Also it should be stated that on the go, data should be stored on the password protected USB devices.

When an individual if fired or leave an organisation, his permissions, privileges and emails should be cut off almost immediately. All the devices by the individual should be accounted for and collected as when he leaves like the mobile phone, laptops, proprietary software and data.
Also, regularly account passwords should be updated, accounts of ex-employees deleted, and access to VPN and email systems revoked.

OUTSIDERS

1. Spear phishing

Phishing are attempts to acquire sensitive information, by imitating to be a trust worthy entity through any sort of communication. Usually phishing is done through sending emails or IMs, which the victim perceives as being genuine.

A phishing attack mainly aims at:

a) Identity theft
b) Retrieving account details
c) Bank account details

These messages contain certain links which when clicked grab the browser cookies. With the help of these, the attacker can access the victim's accounts and cause the kind of destruction he wishes. Phishing links might also take the victim to such web pages which ask him to enter a few details; these might reveal the victim to the attacker.

As an employee of a company, if the account of victim contains any sensitive information of the company, this would cause damage to the company. Therefore employees should have access to only company emails in the office. The mails should be watched for data theft or any other illegal activities also.

A good firewall and secure web browsing software should be in place. Browsers should be up-to-date. Employees should be educated about such attacks and should be asked to judiciously provide their details at various websites visited by them.

2. Infection via a Drive-By Web Download

Many times while browsing for information on the internet we encounter certain documents that we wish to download for future references. Apart from these, many a times, we are redirected to sites which ask us to download a few softwares to proceed. If these are free, there are chances that they might contain hidden malicious codes which we call malwares, which may infect the system which might not only lead to data loss but may also expose any sensitive data to attacker who can make unethical use of it. Company may face not only financial but also reputational damages which are hard to recover.

Again to prevent this, updated firewall and secure web browsing software should be in place. Restricted sites should be open for surfing in the company premises to not only prevent such incidents but also to improve employee performance.

3. USB key malware

With time USB devices have become very popular for storing large data, up to 20 gigabytes in a small device. They are literally everywhere today, and according to the security expects, that is exactly what is creating the problem. Their fears aren't unfounded.

USB storage devices have gotten so popular, cyber criminals are starting to write viruses and worms that specifically target them. That's dangerous because if someone plugs an infected USB drive into their office network the worm can upload and replicate itself on the network.

Another risk associated with the USB drives is that, they can be misplaced easily because they are very small in size, and if by chance the lost device contains sensitive or personal data, a lot of harm can be caused.

Ways to counter such threats are:

a) Limit or rather ban the use of all personal removable media devices except the ones which have been approved by the organisation's chief IT security officer
b) Any data on the USB device should be encrypted
c) Storing sensitive or personal information on the USB device should be avoided
d) Consider the costs and benefits of distributing locked-down, corporate-controlled devices over implementing a "bring your own device" policy
e) Proper antivirus softwares should be installed in the systems, which automatically scan the connected potable device for any malware
f) The devices should be protected using passwords
g) Any missing device should be reported immediately, so that data can be wiped off remotely

4. Scanning networks for Vulnerabilities and Exploitment

The corporate network can be vulnerable to some of the most common exploits and entry points used by intruders to access organizational network resources. Some of these exploits are:

a) *Null or default passwords*

Leaving administrative passwords blank or using a default password set by the product vendor can make the network vulnerable as it can be accessed by any unauthorized user as well.

b) *Default shared keys*

Secure services sometimes package default security keys for development or evaluation testing purposes. If these keys are left unchanged and are placed in a production environment on the Internet, any user with the same default keys has access to that shared-key resource, and any sensitive information contained in it.

c) *IP spoofing*

A remote machine acts as a node on the company's local network, finds vulnerabilities in the servers, and installs a backdoor program or Trojan to gain control over the network resources. Once this is done, all the data moving across the network can be accessed by the attacker.

d) *Eavesdropping*

It is a process by which data that passes between two active nodes on a network is collected by eavesdropping, on the connection between the two nodes.

e) *Service vulnerabilities*

An attacker finds a flaw or loophole in a service run over the Internet; through this vulnerability, the attacker compromises the

entire system and any data that it may hold, and could possibly compromise other systems on the network.

f) *Application vulnerabilities*

Attackers find faults in desktop and workstation applications such as e-mail clients and execute arbitrary code, implant Trojans for future compromise, or crash systems. Further exploitation can occur if the compromised workstation has administrative privileges on the rest of the network.

g) *Denial of Service attack (DoS)*

Attacker or a group of attackers coordinate against an organization's network or server resources by sending unauthorized packets to the target host (either server, router, or workstation). This forces the resource to become unavailable to legitimate users.

5. Social Engineering passwords

All the Social Engineering methods of attack target some very natural human attributes. Some of the Tactics are:

- Trust (Direct approach, Technical expert)
- The desire to be 'helpful' (Direct Approach, Technical expert, Voice of Authority)
- The wish to get something for nothing (Trojan horse – chain email)
- Curiosity (Trojan horse – open email attachments from unknown senders)
- Fear of the unknown, or of losing something (Popup window)
- Ignorance (Dumpster diving, Direct Approach)
- Carelessness (Dumpster Diving, Spying and eavesdropping)

Measures to reduce the impact of social engineering:

- A well-documented and accessible Security Policy with a training given to the employees on it
- Awareness of threats and impact of social engineering on the company
- Operating procedures to limit vulnerabilities
- Use of physical technical solutions 'intelligent revolving doors', biometric systems, to eliminate or reduce unauthorized physical access
- Cost mitigation with insurance protection

6. Wi-Fi compromises

Free Wi-Fi has become a great attraction these days. From shopping malls to cafes to airports, customers expect free Wi-Fi everywhere these days and failing to provide this can cost business a lot of competition.
However, providing free Wi-Fi can risk company network too. It creates a threat to the secure company network as it is open for all users. By using various tools such as 'Cane & Able' and 'Wireshark' which grab the data broadcasted by the Wi-Fi making the network unsecure. If the data broadcasted by the Wi-Fi is not encrypted, the risk increases manifolds.

With Service Set Identifier (SSID) technology, the company can set up two separate points of access to the network: one private and secure for the employees and one available to guests and customers. A private network allows employees to instantly share important documents–without compromising security. This set-up makes Wi-Fi service available to your visitors while keeping the business information safe and confidential.

7. Stolen credentials from third party sites

A credential is an attestation of qualification, competence, or authority issued to an individual by a third party with a relevant or de facto authority or assumed competence to do so. A person holding a credential is usually given documentation or secret knowledge (e.g., a password or key) as proof of the credential. Sometimes this proof (or a copy of it) is held by a third, trusted party.

In Business, credentials represent real-life experience. Companies typically represent their credentials (or "creds") via business citations which describe each successful implementation of a product or service for a customer. A company's credentials are an important factor for Buyers of products or services in making decisions regarding potential vendors who have the most appropriate experience to meet their business needs.

All hackers do not attack all types of corporate credentials. Then who attacks what?

- For organized crime, that is, primarily financially motivated, hackers go after payment cards, credentials and bank account info stored at POS terminals and databases
- For state-affiliated crime, hackers target manufacturing, professional and transportation organizations seeking credentials, internal data and trade secrets stored on file, mail or directory servers
- For activist crime, attackers target web apps, databases and mail servers containing personal info, credentials, and internal data from information, public and other services

The credentials can be stolen in three major ways:

- Key-loggers malwares

- Phising
- Hacking of e-commerce websites

One has to take certain prevention steps in order to be safe from credential theft. The possible ways are:

- Sensitive applications should not be logged into from unprotected machines
- One should be caution about the spear-phising emails
- Passwords should be changed regularly and same credentials should not be used across multiple systems
- Preferably two step verification should be used which adds to user information cutting down the risk of compromise

8. Compromised web-based Databases

Web-based Databases have the following vulnerabilities:

- ✓ Excessive privilege abuse
- ✓ Legitimate privilege abuse
- ✓ Privilege elevation
- ✓ Exploitation of vulnerable, misconfigured databases
- ✓ SQL injection
- ✓ Malware
- ✓ Denial of service
- ✓ Database communication protocol vulnerabilities
- ✓ Unauthorized copies of sensitive data
- ✓ Backup data exposures

Gain to any sensitive data due to the above reasons can cost a lot to the company. Unfortunately, the cost of data breaches is very high and with its analysis it is necessary to adopt proper steps to mitigate the risk of cyber-attack.

IT experts suggest adopting multi-layered security defense strategy to reduce the above risks.

9. Exploiting password reset services to hijack accounts

Password recovery functionalities can result in vulnerabilities in the same application they are intended to protect. Vulnerabilities such as username enumeration (showing different error messages when the user exists or not in the database), sensitive information disclosure (sending the password in clear-text by e-mail to user) and recover password message hijack (involving an attacker receiving a copy of the recover password message) are some common vulnerabilities that may be found in a password recovery functionality. Various developers don't take into consideration the real implications of unsecure password recovery.

Good password recovery functionality generates a token and sends this token by e-mail to the user as a one-time password recovery method (commonly as a link). This token should have the following characteristics:

- have at least 64 characters in length
- be unique
- be random
- be one-time use only
- have a short life (expire in 24hr or less)

When a user clicks the link, the application must check if the token is valid. If so, the application must invalidate the token so it can't be reused and allow the user to change his password. Furthermore, if a user attempts to recover their password a second time before completing the recovery process the first time, the application must invalidate the old password request and generate a new one.

WEB SITE VULNERABILITIES

Today, many big businesses have expanded across the globe, and all their data is stored online on their personal clouds and websites. This results in a major risk of a Data Breach if the web sites are not secure, i.e. have vulnerabilities. Common web site vulnerabilities are:

1. SQL Injection

SQL injection attacks attempt to use application code to access or corrupt database content. This is accomplished via a Web request where the Web user input is incorrectly filtered for string literal escape characters that can be embedded in your SQL statements (like " or *) or more generally not strongly typed or sanitized, and thereby unexpectedly interpreted and executed as SQL.

2. Cross-Site Scripting (XSS)

Often used in conjunction with phishing, social engineering, and other browser exploits, XSS attacks inject malicious HTML or client-side scripts into Web pages viewed by other users, thereby bypassing access controls that browsers use to make sure requests are from the same domain (same origin policy).

By these means, an attacker can gain elevated access privileges to sensitive page content, session cookies, and a variety of other client-side objects through a XSS attacks. Some XSS attacks can be tracked to DOM-based or local cross-site script vulnerabilities within a page's client-side script itself, often called non-persistent or reflected XSS vulnerabilities.

3. Session Fixation

Session Fixation is an attack technique that forces a user's session ID to an explicit value. Depending on the functionality of the target web site, a number of techniques can be utilized to "fix" the session ID value. These techniques range from Cross-site Scripting exploits to peppering the web site with previously made HTTP requests. After a user's session ID has been fixed, the attacker will wait for that user to login. Once the user does so, the attacker uses the predefined session ID value to assume the same online identity.

Without active protection against Session Fixation, the attack can be mounted against any web site that uses sessions to identify authenticated users. Web sites using sessions IDs are normally cookie-based, but URLs and hidden form fields are used as well. Unfortunately, cookie-based sessions are the easiest to attack. Most of the currently identified attack methods are aimed toward the fixation of cookies.

4. Information Leakage

Camouflage should be "standard issue" for Web servers. The first task of a Web attacker (a cyber-criminal, internal or external) is to determine your operating system, Web server, application server and database platforms.

The most successful attacks are often targeted attacks, so removing or obfuscating the signatures of your technology platforms -- both obvious ones like the server name header or file extensions in HTTP, or the TCP/IP window size, as well as more subtle signatures, like cookie names, ETag formats, HTTP header order, or services running on IP/port combinations -- is an important type of countermeasure in itself.

This can either dissuade intruders from attacking your Web site or Web application altogether or force them to make incorrect assumptions that lead them to try the wrong types of attacks (for instance, a Linux/UNIX

hack on a Windows system). In turn, this makes it easier for firewalls and IDS systems to better identify and block those attacks directly.

5. Remote File Inclusion (RFI)

Remote File Include (RFI) is an attack technique used to exploit "dynamic file include" mechanisms in web applications. When web applications take user input (URL, parameter value, etc.) and pass them into file include commands, the web application might be tricked into including remote files with malicious code.

Almost all web application frameworks support file inclusion. File inclusion is mainly used for packaging common code into separate files that are later referenced by main application modules. When a web application references an include file, the code in this file may be executed implicitly or explicitly by calling specific procedures. If the choice of module to load is based on elements from the HTTP request, the web application might be vulnerable to RFI.

6. Brute Force

A, B, C, D, Admin Access... A brute force attack, sometimes called a dictionary attack, is a method of defeating a cryptographic authentication/authorization scheme by trying a large number of possible answers. The best example is exhaustively working through all possible keys in order to discover a password combination.

Like a zero day attack, brute force attacks are often used to find open, unprotected directories or to break authentication and authorization layers. Effective request throttling, tracking and limiting the frequency of Web requests per second to a particular login file or directory, often defeats this form of automated attack.

7. Cross-Site Request Forgery

Cross-site request forgery (CSRF or XSRF), also known as a one click attack or session riding, is an exploit very similar to an XXS attack. Rather than an attacker injecting unauthorized code into a Web site, a cross-site request forgery attack only transmits unauthorized commands from a user that the Web site or application considers to be authenticated.

At risk are Web sites and applications that perform actions based on input from trusted and authenticated users without requiring the user to authorize the specific action. These attacks are characteristic vulnerabilities of Ajax-based applications that make use of the XMLHttpRequest (XHR) API. A user that is authenticated by a cookie saved in his Web browser could unknowingly send an HTTP request to a site that trusts him and thereby cause an unwanted action (for instance, withdrawing funds from a bank account).

8. Denial of Service

Denial of Service (DoS) is an attack technique with the intent of preventing a web site from serving normal user activity. DoS attacks, which are easily normally applied to the network layer, are also possible at the application layer. These malicious attacks can succeed by starving a system of critical resources, vulnerability exploit, or abuse of functionality.

Many times DoS attacks will attempt to consume all of a web site's available system resources such as: CPU, memory, disk space etc. When any one of these critical resources reach full utilization, the web site will normally be inaccessible.

As today's web application environments include a web server, database server and an authentication server, DoS at the application layer may target each of these independent components. Unlike DoS at the network layer, where a large number of connection attempts are required, DoS at the application layer is a much simpler task to perform.

9. Insecure Direct Object Reference

A direct object reference is when a developer exposes a reference to an internal implementation object, such as a file or directory, as a URL or form parameter. An attacker can manipulate direct object references to access other objects without authorization.

10. Insecure Cryptographic Storage

Web applications that do not use appropriate encryption for sensitive information such as social security numbers and credit card information leave users open to a compromise in the event of an attack. Organizations should take stock of the threat landscape and make sure sensitive data is protected. Also off-site backups should be encrypted, with the keys managed and stored separately.

TYPES OF MALWARE ATTACKS

Malware Attack is the initial small step, which when executed correctly, leads to the final devastation in the form of a Data Breach or a Cyber-Crime. The main types of Malware Attacks which are prevailing as of today are:

1. ***Adware***: The least dangerous and most lucrative Malware. Adware displays ads on your computer.

2. ***Spyware***: Spyware is software that spies on you, tracking your internet activities in order to send advertising (Adware) back to your system.

3. ***Virus***: A virus is a contagious program or code that attaches itself to another piece of software, and then reproduces itself when that software is run. Most often this is spread by sharing software or files between computers.

4. ***Worm***: A program that replicates itself and destroys data and files on the computer. Worms work to "eat" the system operating files and data files until the drive is empty.

5. ***Trojan***: The most dangerous Malware. Trojans are written with the purpose of discovering your financial information, taking over your computer's system resources, and in larger systems creating a "denial-of-service attack" Denial-of-service attack: an attempt to make a machine or network

resource unavailable to those attempting to reach it. Example: AOL, Yahoo or your business network becoming unavailable.

6. ***Rootkit***: This one is likened to the burglar hiding in the attic, waiting to take from you while you are not home. It is the hardest of all Malware to detect and therefore to remove; many experts recommend completely wiping your hard drive and reinstalling everything from scratch. It is designed to permit the other information gathering Malware ~~in~~ to get the identity information from your computer without you realizing anything is going on.
7. ***Backdoors***: Backdoors are much the same as Trojans or worms, except that they open a "backdoor" onto a computer, providing a network connection for hackers or other Malware to enter or for viruses or SPAM to be sent.

8. ***Keyloggers***: Records everything you type on your PC in order to glean your log-in names, passwords, and other sensitive information, and send it on to the source of the keylogging program. Many times keyloggers are used by corporations and parents to acquire computer usage information.

9. ***Rogue security software***: This one deceives or misleads users. It pretends to be a good program to remove Malware infections, but all the while it is the Malware. Often it will turn off the real Anti-Virus software. The next image shows the typical screen for this Malware program, Antivirus 2010

10. ***Ransomware***: If you see this screen that warns you that you have been locked out of your computer until you pay for your cybercrimes. Your system is severely infected with a form of Malware called Ransomware. It is not a real notification from the FBI, but, rather an infection of the system itself. Even if you pay to unlock the system, the system is unlocked, but you

are not free of it locking you out again. They request for money, usually in the hundreds of dollars which is completely fake.

11. ***Browser Hijacker***: When your homepage changes to one that looks like those in the images inserted next, you may have been infected with one form or another of a Browser Hijacker. This dangerous Malware will redirect your normal search activity and give you the results the developers want you to see. Its intention is to make money off your web surfing. Using this homepage and not removing the Malware lets the source developers capture your surfing interests. This is especially dangerous when banking or shopping online. These homepages can look harmless, but in every case they allow other more infectious

12. ***Denial-of-Service Attack***: A denial-of-service or a DOS attack generally means attacking the network to bring it down completely with useless traffic by affecting the host device which is connected to the internet. A DOS attack targets websites or services which are hosted on the servers of banks and credit card payment gateways.

13. ***Direct-access Attack***: A direct-access attack simply means gaining physical access to the computer or its part and performing various functions or installing various types of devices to compromise security. The attacker can install software loaded with worms or download important data, using portable devices.

14. ***Eavesdropping***: As the name suggests, eavesdropping means secretly listening to a conversation between the hosts on a network. There are

various programs such as Carnivore and Narus Insight that can be used to eavesdrop.

15. ***Spoofing***: Spoofing is a cyber-attack where a person or a program impersonates another by creating false data, in order to gain illegal access into a system. Such threats are commonly found in emails where the sender's address is spoofed.

16. ***Tampering***: Tampering is a web based attack where certain parameters in the URL are changed without the customer's knowledge; and when the customer keys in that URL, it looks and appears exactly the same. Tampering is basically done by hackers and criminals to steal the identity and obtain illegal access to information.

17. ***Repudiation Attack***: A repudiation attack occurs when the user denies the fact that he or she has performed a certain action or has initiated a transaction. A user can simply deny having knowledge of the transaction or communication and later claim that such transaction or communication never took place.

18. ***Information Disclosure***: Information disclosure breach means that the information which is thought to be secured is released to unscrupulous elements which are not trustworthy.

19. ***Privilege Escalation Attack***: A privilege escalation attack is a type of network intrusion which allows the user to have an elevated access to the network which was primarily not allowed. The attacker takes the

advantage of the programming errors and permits an elevated access to the network.

20. ***Exploits***: An exploit attack is basically software designed to take advantage of a flaw in the system. The attacker plans to gain easy access to a computer system and gain control, allows privilege escalation or creates a DOS attack.

21. ***Social Engineering***: An attack by a known or a malicious person is known as social engineering. They have knowledge about the programs used and the firewall security and thus it becomes easier to take advantage of trusted people and deceive them to gain passwords or other necessary information for a large social engineering attack.

GENERAL DATA SECURITY TIPS

Keeping in mind the common threats faced by the businesses as discussed above, summing up the Top Data Security Tips to Safeguard Your Business would be:

1. GET TO KNOW YOUR ENVIRONMENT

Conduct a security audit to identify the vulnerabilities in your business. If you don't know your points of weakness, you can't properly predict where hackers can gain entry. Audit your entire infrastructure and environment to determine points of vulnerability in your network, your devices, and your employee policies. Make this a regular practice. Cyber threats evolve constantly so you need to audit on a regular basis. Once you know where potential threats may occur, you can take action to protect against them.

2. GET TO KNOW YOUR DATA

Know where your sensitive data resides so you can effectively target your remediation activity in the case of a security breach. Does the developer's laptop contain a blueprint for an upcoming project? Is a salesperson downloading hundreds of files from the corporate network at 3am? A Data Loss Prevention (DLP) tool will help alert you to the presence of sensitive data and will allow you to monitor unusual movements of data.

3. EDUCATE STAFF AND EMPOWER THEM TO BE DATA SECURITY GUARDS

You can decide to view employees as potential points of failure or potential points of security. Educate your employees, empower them, and they can become your first line of defense. Human error is one of the biggest causes of data breaches.

By fostering an environment of vigilance, you can keep security concerns top-of-mind with your employees. Build awareness about the biggest risks such as Adobe Acrobat and Java exploitations, fake antivirus warnings, phishing sites, USB keys disguised as promotional material, and so on.

4. ENFORCE COMPLEX AND FREQUENTLY UPDATED PASSWORDS

This seems very straightforward but too many employees use simple passwords that are easy for hackers to guess. And more frighteningly, many people use the same password for years— and re-use it for all platforms that require a login.

Hackers, or cybercriminals, are persistently on the lookout for data to steal— personal information, healthcare data, financial records, intellectual property and other proprietary information.

Educate your employees, empower them, and they can become your first line of defence. Human error is one of the biggest causes of data breaches.

If passwords are too simple, hackers can employ a 'dictionary attack' which automates the use of a combination of dictionary words and numbers to crack passwords. Make sure employees are aware of this and set password polices that force them to use special characters and change their passwords frequently.

5. COMMUNICATE CLEAR DATA AND DEVICE USAGE POLICIES

With the wave of personal devices and connected 'things' such as wearable entering the workplace, it is important to review BYOD and COPE policies frequently to ensure you are keeping up to date with the latest trends.

Guest wireless networks should be isolated. If an employee device connects to the corporate network, the device should be checked for compliance and directed to a device enrollment page detailing the employee and company rights regarding the management of data.

If employees choose to use a personal device at work, they must accept your BYOD policies. Choose an asset management tool that is capable of managing multiple device types (including desktops and laptops) and ownership models. If a specific device doesn't provide the necessary baseline security requirements, such as on-device encryption, it is reasonable to say no to the employee who wishes to use it. Just be clear about your policies and the devices you will support.

6. USE ENCRYPTION

Data encryption is a must. Encrypt all data that is stored on portable devices including laptops, tablets, and smartphones. If encryption is in place when a device goes missing, whoever accesses the data won't be able to read it. Encryption software will also help you to defend your company against a negligence claim in the case of a data breach—as long as you can prove encryption was in place and working properly at the time of the breach.

7. COMPLEMENT YOUR ENCRYPTION WITH PERSISTENT SOFTWARE

Choose a persistent endpoint security and management solution that will allow you to maintain a connection with a device regardless of user or location. Persistence® technology ensures that security software reinstalls if it is removed or damaged, accidently or on purpose. Persistent security software will also allow you to run encryption and anti-virus status reports so you can prove these solutions are in place and operational at the time of theft.

8. TAKE A LAYERED APPROACH TO SECURITY TECHNOLOGY

There is no Holy Grail of data security software. Hackers have sophisticated methods to gain entry so it is critical to take a layered approach to security technology on all your devices and networks. Multiple security solutions will reduce the threat landscape, prevent advanced attacks on your network and alert you to a persistent threat or any anomaly so you can take the appropriate action.

9. KEEP SOFTWARE UP-TO-DATE

Hackers are experts at exploiting vulnerabilities found in software. Developers release regular patches to plug security holes and it is important that you have an asset management tool in place to ensure that these patches are installed automatically.

Be diligent with your updates and don't wait to install a patch. One inadvertent downside to patching is that it provides a hacker with the code to understand the vulnerability that the patch is intended to repair. With this information, hackers can target devices and systems where the patch has not yet been implemented and exploit the fault to their advantage.

10. BE PREPARED FOR A DATA BREACH

We are all just one mistake away from a crisis. Build a data breach playbook filled with scenarios and response actions. Put escalation levels in place and decide how transparent you want to be about the attack and whether any regulatory bodies or customer groups need to be notified.

In the case of a stolen device or rogue employee, ensure your endpoint security software allows you to perform remote actions such as data delete, data retrieval, device freeze, and, when necessary, launch forensic investigations.

Data is the lifeblood of your organization and it requires time, resources and investment to protect it. With data regulations tightening across all industries, now is the time to act.

NEED OF CYBER LAWS

Information technology has spread throughout the world. The computer is used in each and every sector wherein cyberspace provides equal opportunities to all for economic growth and human development. As the user of cyberspace grows increasingly diverse and the range of online interaction expands, there is expansion in the cyber-crimes i.e. breach of online contracts, perpetration of online torts and crimes etc. Due to these consequences there was need to adopt a strict law by the cyber space authority to regulate criminal activities relating to cyber and to provide better administration of justice to the victim of cyber-crime. In the modern cyber technology world it is very much necessary to regulate cyber-crimes and most importantly cyber law should be made stricter in the case of cyber terrorism and hackers.

LAWS RELATING TO DATA/CYBER SECURITY IN INDIA

The Indian legal system is substantially based on the British common law system. While there is no omnibus Indian data security law, there are several laws that apply to data theft or misuse in India. Typically, when an incident involving data occurs, a complaint is filed for theft, cheating, criminal breach of trust, dishonest misappropriation of data and/or criminal conspiracy under the provisions of the Indian Penal Code, 1860 ("IPC"), and for hacking under the Information Technology Act, 2000 ("ITA"). Many of these offenses under the IPC and the ITA allow for an arrest without a warrant, are non-bailable and carry penalties that range from imprisonment for a year to life imprisonment, as well as fines.

Moreover, certain offenses carry higher penalties when the offender is an employee, a public servant, a merchant, an attorney or an agent. For example, misappropriation of data by criminal breach of trust carries a penalty of imprisonment for up to three years. However, when the criminal breach of trust is carried out by an employee (such as in a case where the data is dishonestly misappropriated and converted by an employee for his or her own use), the penalty increases to imprisonment for up to seven years. Further, when the offender is a public servant, merchant, attorney or agent, the penalty can be as high as life imprisonment.

In addition to these criminal affairs, civil proceedings for copyright infringement under the provisions of the Copyright Act, 1957 ("CA") and the Specific Relief Act, 1963 ("SRA") are also typically initiated to prevent the misuse and dissemination of data. The penalties under the CA and the SRA can range from hefty fines and damages to temporary and permanent injunctions.

CYBER LAWS IN INDIA

Section	Offence	Description	Penalty
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	Imprisonment up to three years, or/and with fine up to₹200,000
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to₹500,000

66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to₹100,000
66C	Using password of another person	A person fraudulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to₹100,000
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to three years, or/and with fine up to₹100,000
66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to₹200,000
66F	Acts of cyber terrorism	If a person denies access to an authorized personnel to a computer resource, accesses a protected system or introduces contaminant into a system, which the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyber terrorism.	Imprisonment up to life.

67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to₹1,000,000
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexual explicit act or conduct.	Imprisonment up to seven years, or/and with fine up to₹1,000,000
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
67C	Failure to maintain records	Persons deemed as intermediary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.

68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who fails to comply with any such order shall be guilty of an offence.	Imprisonment up to three years, or/and with fine up to₹200,000
69	Failure/refusal to decrypt data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the	Imprisonment up to seven years and possible fine.

		information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	
70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to three years, or/and with fine up to₹100,000

ENFORCEMENT PROCEDURES

What do you do if you're in a company that needs to deal with an incident of data misuse or theft in India? In general, you'd start by filing a criminal complaint with the police station that has jurisdiction over the area where the data security breach occurred. This comes under the provisions of the ITA, IPC and CA for theft, misappropriation, or misuse of data and infringement of copyright. The local police station however, may not be in a position to properly investigate a data security incident, as not all officers are adequately trained to deal with cyber-crime cases.

Thus, in the alternative, you can make a criminal complaint to Cyber-Crime Cells set up by the State Police Departments. These Cyber-Crime Cells have been established specifically to investigate and prosecute cases of data theft and copyright infringement, as well as other cyber-crime cases. Cyber-Crime Cells of several State Police Departments (such as Delhi) organize training programs to enhance investigators' skills and knowledge concerning data protection. Plus, they have the know-how to use advanced equipment to investigate data security incidents.

The investigating officers at Cyber-Crime Cells have the power to seize infringing or stolen data by conducting searches and raids on the premises of the alleged offenders and can also prosecute the offenders in the criminal court that has jurisdiction over the police station where the complaint was registered. The law enforcement agencies also have the power to arrest offenders and keep them in custody during the course of the investigation and prosecution (until bail is granted to the offenders by the court).

If a company believes that the local police station and/or the Cyber-Crime Cell lack the requisite expertise to investigate a data security incident, the company may make a formal complaint with the Central Bureau of Investigations (the "CBI") under the provisions of the ITA, IPC and CA. The CBI is an independent, autonomous investigating agency set up by the Government of India, which has professionally trained the Cyber-Crime Units in various states to investigate data security incidents. If the officer investigating the complaint determines that a prima-facie offence is committed, he or she can register the complaint and file a charge sheet with the competent criminal court.

Additionally, complaints alleging offenses under provisions of the ITA can also be made to the Controller of Certifying Authorities. Upon receipt of a complaint, the Controller of Certifying Authorities investigates allegations and can order punishment of an offender under the provisions of the ITA. As the Controller of Certifying Authorities is a quasi-judicial authority, an appeal against its orders can be made only in the State High Court.

Finally, in addition to, or in lieu of, a criminal complaint, under the provisions of the CA and the SRA, you can file a civil suit seeking damages and an injunction to restrain the misuse and misapplication of data. A civil court can issue an interim temporary injunction pending final adjudication of the civil suit.

ARCHITECTURAL FRAMEWORK TO PROTECT THE COMPANY

Gartner has developed an architectural framework composed of four stages and 12 capabilities in the organisation that will help enterprises design an ASA and select from among competing products. The four stages of Gartner's ASA are:

a) Prevent

The company needs a set of policies, products and processes that are put into place to prevent a successful attack. The key goal is to reduce the attack surface and prevent attacks before they can impact the enterprise.

b) Detect

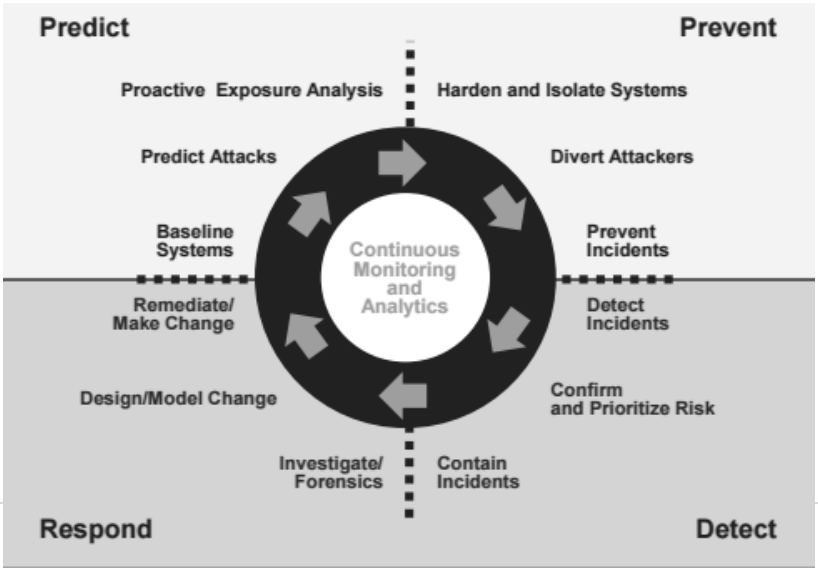
Find attacks that have evaded the prevention layer. The key goal is to reduce the "dwell time" threats and, thus, reduce the potential damage they can cause.

c) Respond

Proficiencies are required to remediate issues discovered by detective activities, provide forensic analysis and recommend new preventive measures to avoid repeat failures.

d) Predict

Modeling allows the security organisation to learn from external events and sources to proactively anticipate new attack types. This intelligence is then used to feed the preventive and detective activities.



CONCLUSION

Security attacks and phishing campaigns are not something new for companies, but only in recent years have they reached this level of sophistication, which got most security analysts saying that a company should prepare for such an issue if it wants to maintain its business and reputation in the online industry.

Even more, the problem with security breaches is that the retrieved data is somehow exposed to the world, which places people in an awkward position of not knowing who to judge, the cyber-thieves or the personal information revealed?

Unfortunately, it is impossible to forecast a data breach. The bottom line is, security breaches will always be a threat. If you follow the steps to protecting yourself then you can lessen your chances of becoming a victim.

REFERENCES

www.us-cert.gov

www.cert-in.org.in

www.symantec.com

Various articles at https://access.redhat.com

Various articles at www.sans.org

Article on corporate credential theft at https://securityintelligence.com

Articles posted on http://resources.infosecinstitute.com

Articles on cyber security on www.forbes.com

HP report namely "HP TippingPoint- A New Approach To Malware Defenses"

http://www.legalindia.com/cyber-crimes-and-the-law/

https://en.wikipedia.org/wiki/Information_Technology_Act,_2000

Whitepaper by ABSOLUTE titled "Top 10 Data Security Tips to Safeguard Your Business"

https://www.dubex.dk/en/update/malware-is-already-inside-your-organisation-deal-with-it/