NETRIKA
CONSULTING & INVESTIGATIONS

CYBER SECURITY PREPAREDNESS SURVEY

- by Netrika Consulting

Cyber Security Preparedness Survey - Are we Ready?

In the absence of comprehensive cyber security, cyber threats can wreak havoc on businesses in seconds, as the time from knowledge of vulnerability to release of exploit is shrinking. And yet, many organizations remain ill-equipped to handle security attacks as they happen across platforms.

An eye-opening survey on cyber security situation in corporate world carried by NETRIKA CONSULTING.

Supporting Associations

ASIS INTERNATIONAL
Advancing Security Worldwide®

ICCA
INDIAN CORPORATE COUNSEL ASSOCIATION

Disclaimer

Netrika Consulting has exercised due care and diligence in preparing this book. However, the information contained is of judicial nature and has been compiled or arrived at from sources believed to be reliable, but no representation or warranty is made to their accuracy, completeness or correctness and hence, Netrika Consulting & Investigation cannot be held responsible for any omissions or errors.

This book is for information purposes and to initiate a debate or dialogue concerning matters contained in it. The information contained in this document is published for knowledge and cannot be considered as or a substitute for professional, technical or legal advice.

Readers are encouraged to inform the project partners about any inaccuracies or to provide additional information for future editions.

Cyber Security Preparedness Survey - Are we Ready?

Edition
First, 2018

Key Message

Mr. Sanjay Kaushik
Managing Director
Netrika Consulting & Investigation

With increasingly networked environment and advancement in digitalization newer attack surfaces are emerging thereby leading to increase in sophisticated cyber-attacks. Today cyber threats have already become biggest concern, larger than technological change, uncertain economic growth and terrorism for most of the CEO's across the world.

From the global ransomware attacks that hit hundreds of systems top phishing and scanning rackets, at least one cybercrime was reported every 10 minutes in India in the first six months of 2017. That's higher than a crime every 12 minutes in 2016.

Organizations across sectors have recognized the need and importance of cyber security. Companies have realised it is no more only a IT problem and the onus of protecting critical company resources from a cyber-attack is every body's responsibility from basement to boardroom.

We can no longer view security as a cost center and should consider it as an investment for future success of the organisation. We should aim at creating a culture within the organisation at all the levels and create a human firewall which will help us to protect us against global cyber threats.

Cyber-attacks are inevitable and companies have no option but to prepare themselves to respond to the attacks appropriately. It is high time we should realise that when it comes to cybersecurity, complacency is our biggest enemy. Today there is hyper awareness surrounding cyber security but still we have been hearing breaches and their effects on our organisations and thereby country's economy.

We should be moving from a passive approach towards cyber security to more active approaches of threat hunting, knowing our enemy or go one step ahead towards thinking like criminals if we got to really matchup with them.

However, while doing so basic hygiene towards security should not be compromised as we have seen biggest of cyber-attacks were caused due to very small or basic technology errors or unintentional people giving away vital information due to inadequate awareness towards security.

This book guides corporates on where are they lacking; the applicable laws and acts in India and abroad; how to take preventive and corrective measures; Cybersecurity Best Practices & Cyber Security Essentials; Future Learnings from some famous cyber-attacks which affected Corporate India and rest of the world.

Foreward

Mr. Nitin Chandurkar
Executive Director (IT),
MAHAGENCO - Maharashtra
State Power Generation Co. Ltd.

I would like to congratulate Netrika team for taking this initiative of creating a well-documented survey report on the situation of cyber security preparedness in corporate India.

Technology has touched human lives to an enormous extent. The size of devices is shrinking; Micro devices have taken over erstwhile computers. We have seen a transition from computers to laptops, laptops to tablets and from tablets to mobile phones; which is doing all our day to day tasks of personal banking, bill payments, emails, etc. With this advancement of technology in our lives, it is not uncanny that incidents of technology breaches are on a high. We also read about Crime As a Service, Ransomware as a Service which is really very serious threat to the industry. So we should be well prepared for a crisis before it comes to us in real and then we start preparing ourselves which will be obviously very late.

Corporate sectors are doing various things in the area of cyber security. However, we should be working towards the roadmap of Information Security and have a constant engagement from senior leadership, measure the progress, improve year on year in our capacity to defend ourselves from cyber-attacks as the criminals will be always be one step ahead. In the process we should aim at utilizing our existing resources, upgrading to best in class security solutions with the partnership with our close and trusted partners, learn from mistakes and remain up the curve.

I support the vision of the government to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors of the Nation.

Apart from the precautionary measures taken by the various entities through technical implementations, the major role is required to be played by individuals to protect the information asset. Better participation from the individuals in securing the information asset can be achieved by conducting regular Cyber Security Awareness Training in the organizations and educating all about the Cyber Security aspect.

As a responsible citizen, one has to take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification and raising information security awareness among all stakeholders.

Some of the preventive measures Corporate entities can take is do a security gap assessment and not just check in the box audits, document your information security policies and procedures, ensure they are implemented and does not just remain as books in drawers, carry out employee trainings frequently, measure the response by conducting enough mock drill exercises, carry out technology testing etc.

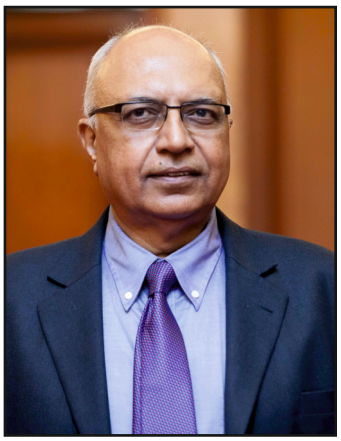
Extending my best wishes to the entire Netrika team.

Foreward

I am delighted to congratulate Netrika Consulting India Pvt Ltd on its Cyber Security Survey Lunch, I commend Netrika for its ongoing commitment in the field of cyber security, and I am confident that its exceptional solutions will continue to serve as a catalyst for success, strengthening individual business.

Netrika is a growing organization that's making its mark in the cyber security field. Theya are making high efforts in building a platform that will be customized to fulfill all cyber security needs. Which enables patrons to take the benefit of the richness of the diversified Cyber Security Platform. At the end I would like to thank Netrika for it's hard work and dedication.

Please accept my best wishes for continued growth and prosperity in the years ahead.



Mr. Ashok Sharma

Founder President, ICCA
Fellow, Chartered Institute of Arbitrators (London)

Foreward

Netrika Consulting is launching the “Cyber Security Preparedness Survey”. This is a great initiative and a step in the right direction; this initiative will lay the foundation of establishing the core essence of a cyber-secure ecosystem not only in organizations but equally society and country at large.

Mr. Manish Datta
Chairperson- ASIS New Delhi Chapter # 207

Most of us are speaking about "Digital India”. Cyber Security Preparedness Survey should assist in defining the security strategy required both in macro and micro terms so as to be able to build an effective cybersecurity model to combat threats. Some of the critical elements as part of preparation and tackling cyber-threats is to educate, raise awareness and establish information sharing platform or forum including reporting for all the critical sectors of the society and industry vulnerable to attacks. Such collaborative initiatives will ensure that we are sharing information and also sharing best practices and models to detect threats and incorporate robust mitigating measures.

I wish the entire team of Netrika Consulting all the very best on the launch of the “Cyber Security Preparedness Survey” program!

Contents

Chapter

1

What is Cyber Security

"Threat is a mirror of security gaps. Cyber-threat is mainly the reflection of our weaknesses. An accurate vision of digital and behavioural gaps is crucial for a consistent cyber-resilience."
—Stephane Nappo, CISO of the year 2018

The term Cyber Security, by default, comprises technologies, processes and controls that are designed to protect systems, networks and data from cyber-attacks. Effective cyber security reduces the risk of cyber-attacks and protects organisations and individuals from the unauthorised exploitation of systems, networks and technologies.

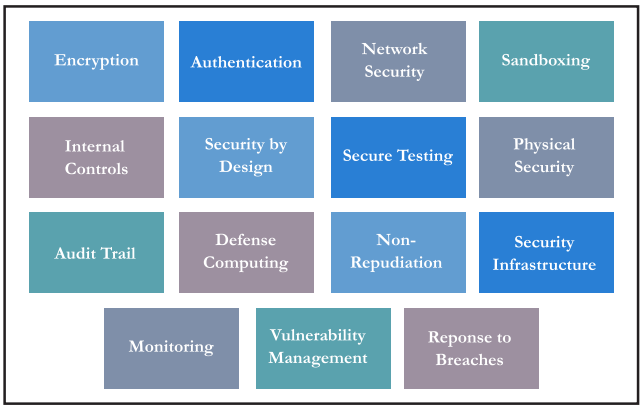
Cyber Security is referred to a set of techniques used to protect information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. Cybersecurity strategies include identity management, risk management and incident management.

Cyber / Security (noun)

"the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this" – **defined by the oxford dictionary.**

The Information Technology Act, 2000 defined cyber security as ***"Cyber Security means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction".***

Examples of cybersecurity are:

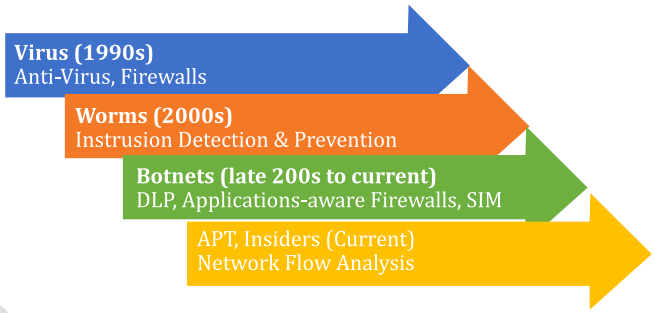


The objective of cybersecurity is to prevent or mitigate harm to – or destruction of – computer networks, applications, devices, and data. The core functionality of cybersecurity involves protecting information and systems from major cyberthreats. These cyberthreats take many forms (e.g., application attacks, malware, ransomware, phishing, exploit kits).

Evolution of Cyber Security

Revolution of digitalization exposed to new types of cyberattacks over the period. From early 90s to till now

cyberattacks took different shapes resulting into higher losses of data and privacy. In the same line cybersecurity was also revolved during past 3 decades. New methods of security were also developed to fight with attacks. The revolution is depicted below:



"Cyber space is the new world. In coming years, humans are going to use it for their survival, same as oxygen & water. When the lives are going to be dependent on it, keeping this new world safe from threats, perceived or evident, will no more be an option. Security of the Cyber space isn't anymore the concern of only few specialists but a domain that screams out for all-inclusive participation. Corporate, Government, Defence, Medical Care, Judiciary, no sector can ill afford a compromise on this count. It's high time, Cyber Security was addressed with all seriousness it deserves & there is no other option but to seek involvement of all stakeholders, working in tandem, with the sole purpose of outsmarting the moves of unscrupulous elements even before an idea of causing harm gets conceived in their minds.

– Lt Col Rajan Agarwal
Ex-Registrar,
The Cyber Appellate Tribunal, New Delhi

"As we've seen recently with Kerala flood and dust storm across north India, natural disasters can have a devastating impact on families, homes, and businesses. However, we have to keep in mind that human-caused hazards, such as cyber-attacks, pose a very real threat as well to people and businesses around the world. The volume and severity of attacks over the past year, organizations are no longer asking if they can be attacked; rather, they are asking how they will be attacked. Realizing that the perimeter is rapidly weakening, organizations are waking up to a reality where the security battlefield is playing out inside their network.

A fading perimeter, combined with the transition to the cloud and deployment of myriads of IoT devices, mean that the attack surface is expanding. The risks for organizations are increasing greatly, as standards and policies fail to keep up. At this point, even consumers are worrying. It is therefore critical that in addition to initiatives in safeguarding IT infrastructure against external/ internal cyber-attacks, Organization should also prepare a framework to respond to cyber-security incidents if and when they occur. The cyber-security incident management framework should sketch roles, responsibilities and steps that various organization personnel, partners and service providers are expected to play in the event of a cyber-security incident."

– Mr. Madan Mohan
Head – Information Security Governance and Compliance,
Idea Cellular Ltd.

Chapter 2

Cybercrime

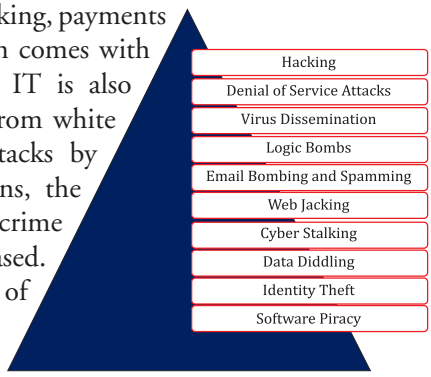
We live in a world where all wars will begin as cyber wars... It's the combination of hacking and massive, well-coordinated disinformation campaigns.

—**Jared Cohen**

Oxford dictionary define cybercrime as *"Criminal activities carried out by means of computers or the Internet"*.

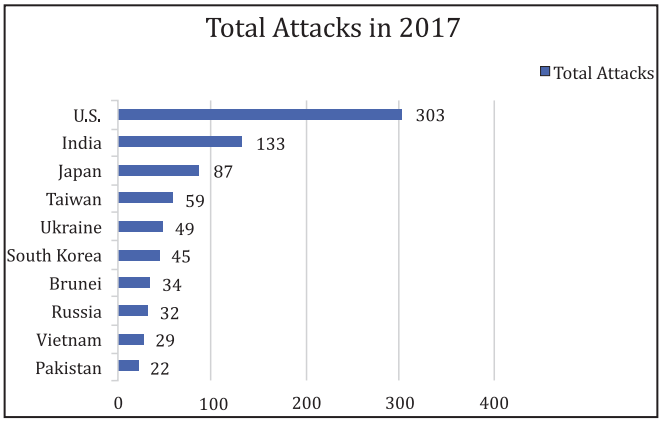
Cybercrimes can be committed in two ways:

The information technology revolution has digitalised everything and provided easy access to users. Life has made very easy and fast due to internet; and everything is just a click away. The technology made population dependent for shopping, travel booking, payments etc. Every revolution comes with some demerits and IT is also not an exception. From white collar crimes to attacks by terrorist organizations, the number of cybercrime cases has also increased. Some examples of cybercrimes:



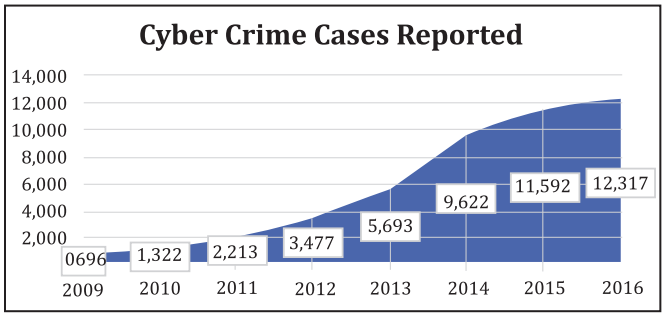
Cybercrimes in India

With the advancement of the technology, abuse has also increased. Other crimes like kidnapping, fraud, hacking, data theft have been committed with the help of internet now. Criminals who perform such activities are often referred as "hackers". From the global ransomware attacks that hit hundreds of systems top phishing and scanning rackets, at least **one cybercrime was reported every 10 minutes in India** in 2017. That's higher than a crime every 12 minutes in 2016. According to the Indian Computer Emergency Response Team (CERT-In), 53,081 security incidents were handled by the team during the year 2017.

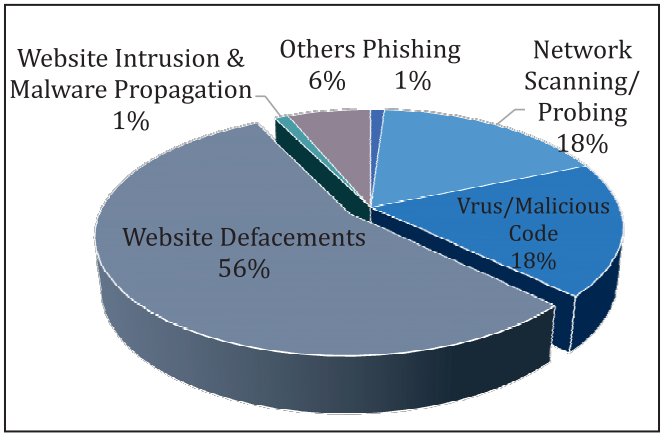


India has emerged one of the soft targets for cybercrime due to rapidly increasing use of technology. Government support for mobilisation and digitalisation increase millions of technology users which include corporates as well as individuals. Lack of awareness about cybersecurity, Indian organisations are on hitlist of hackers. According to Internet Security Threat Report, March 2018 (Symantec), India is the second most country who is affected by cybercrimes after USA.

According to National Crime Reporting Bureau report 2016, cyber-crimes in India are increasing with CAGR of 41% during past 5 years.



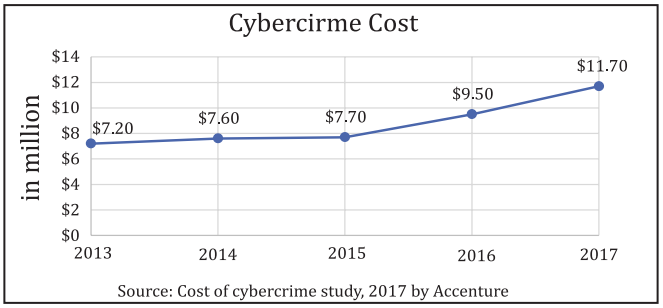
These include phishing, scanning or probing, site intrusions, defacements, virus or malicious code, ransomware and denial-of-service attacks. With more Indians going online, cyber experts said putting in place critical infrastructure to predict and prevent cybercrimes was crucial. Breakup of security incidents handled by CERT is:



The government of India is making efforts to reduce the cyberattacks via awareness and forming special cell such as CERT. However, efforts of the government are also not enough as cybercrime affecting hundreds of individuals as well as commercial systems, who all need to be ready for such attacks. In recent time, while India was involved in whipping crimes such as phishing and defacement, ransomware attacks have come as a bombshell. India is also one of biggest target of ransomware attack. WannaCry, NotPetya, SamSam are the recent examples of ransomware which impacted India badly.

Cybercrime Cost

The financial effect of rapidly growing cybercrimes is becoming worse. According to cost of cybercrime study conducted by Accenture, average global cost of cybercrime was US$11.7 million which was increased 27.4% from 2016.



Source: Cost of cybercrime study, 2017 by Accenture

Average cost of cyberattack in India was approx. US$1.17 million while ransomware contributed approx. US$ 13,300 in total cost of cyber-attacks.

According to Juniper Research global cybercrime cost is estimated to reach at US$2 trillion by 2019.

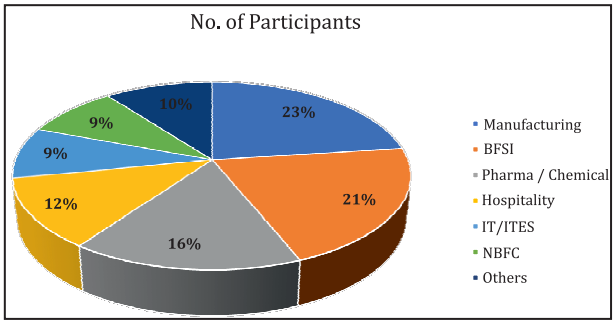
This increasing financial impact of cybercrime need to be taken seriously and organisations need to put intensive efforts to implement cybersecurity seriously. Presently, most of the of organisations are considering cyber security as a compliance and these organisations are very vulnerable to the cyberattack.

Chapter 3

Survey Results

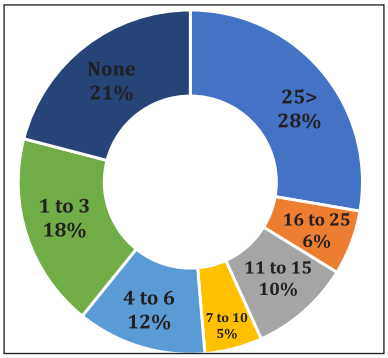
Netrika took the increasing threat of cybercrime seriously and conducted a detailed survey to understand awareness about cyber-crime and security across the industries.

Leading participants in the survey were from manufacturing industry (23%), followed by BFSI (21%), Pharmaceuticals (16%), Hospitality (12%), NBFC (9%), and IT/ITES (9%)

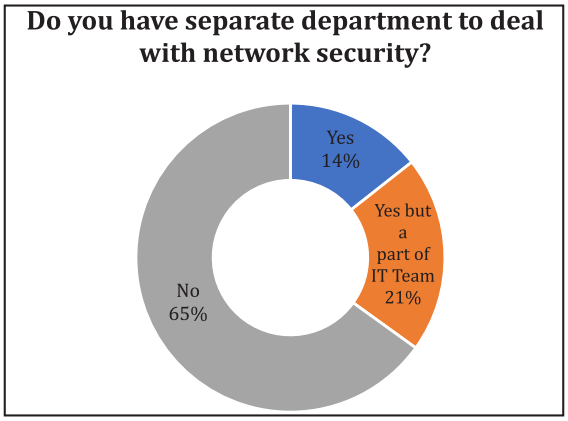


The key reason of successful cyberattacks on corporates is lack of robust IT security system in the organisation. According to the survey, **only 18% organisations have dedicated staff of IT where more than 25 persons are employed while 21% organisations do not have dedicated IT staff.** It is also revealed that 18% organisations have IT strength of 1 to 3 employees.

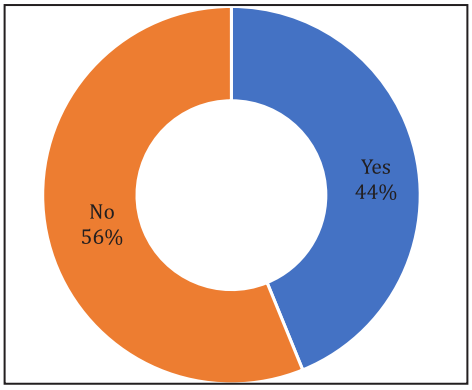
Further, organisations also do not have dedicated staff for cyber/network. The survey revealed that 65% of the participant organisations does not even have department



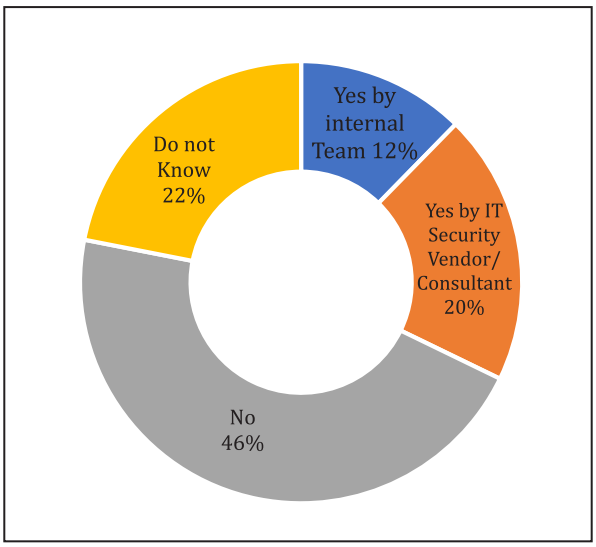
to manage network security while 35% of the participant organisations have department to manage network security which include 14% organisations who have separate department to manage network security and 21% organisations have department which is a part of IT team.



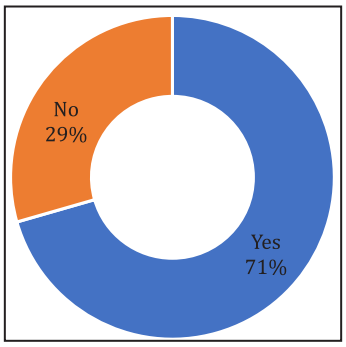
Have you done an IT Security Audit in the last 6 months? Indian corporates are not very regular in assessing their cyber security which leads to regular loss due to cyberattacks, During the survey, 44% participants confirmed that they conduced IT security audit in last 6 months in their organizations while 56% participants stated that during last six months no IT security audit was conducted in their organisation.



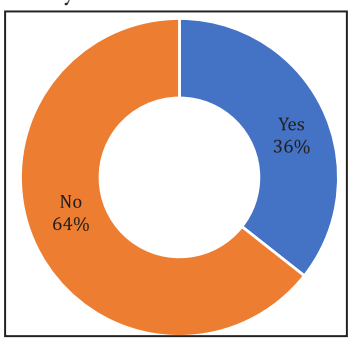
Have you conducted Penetration testing in the last 1 year? The survey revealed that in the last one year 32% participant organisations have carried out penetration testing (by their internal team 12% and by IT security vendor/consultants 20%) while 46% participant organisations have not carried out penetration testing in the last 1 year.



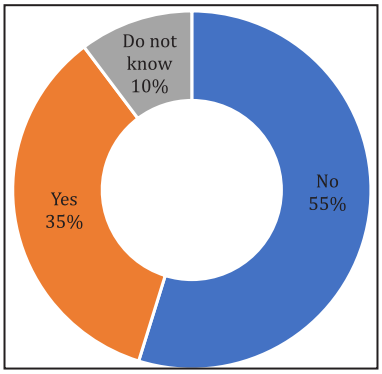
Do you have Information Security Policy and Procedure Manual? The survey revealed that 29% of the participants organisations have security policy and procedure manual while 71% of the participant organisations do not have security and procedure manual.



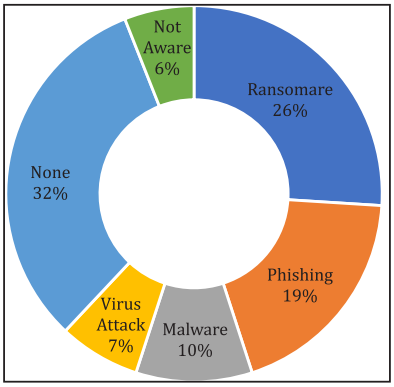
Do you have a Business Continuity Plan in place? During the survey, it was identified that 36% of the participants organisations have business continuity plan while 64% participant organisations does not have Business Continuity Plan.



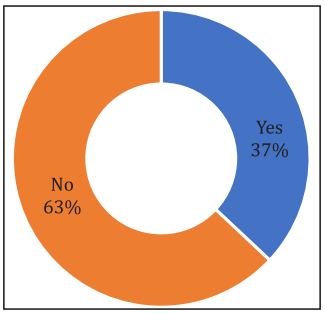
Have you conducted a business continuity mock drill, simulation exercise in last 6 months? The survey revealed that 35% of the participant organisations have carried out business continuity mock drill in the last 6 months while 55% of the participant organisations have not conducted such activity in their organisation in past 6 months any business continuity mock drill.



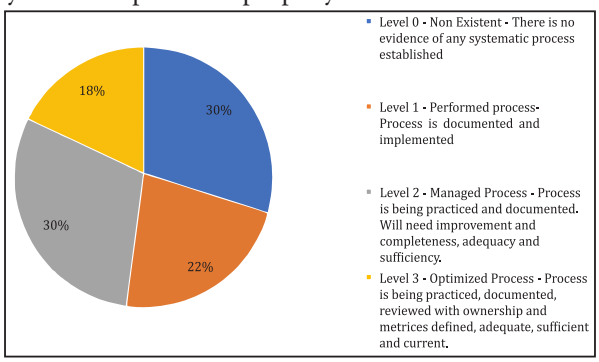
Have you suffered a breach in the last 12 months? Non-assessing the security controls resulting into cyber attacks in the organisations. During the survey 62% participants organisations accepted IT breach in the form of virus attack (7%), malware (10%), phishing (19%), ransomware (26%) while 32% participant organisations have not suffered any breach in the past 12 months.



Information Security Awareness Training in the last 12 months? The survey revealed that 37% organisations conducted information security awareness training in past 12 months, however, 63 organisations are not regular in such trainings.



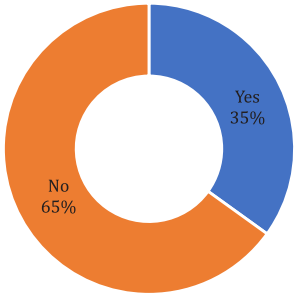
The survey revealed that 30 % of the participant organisations does not have any systematic process with respect to IT security, 22% of the participant organisations have the process documented and implemented, however, they have not practiced properly.



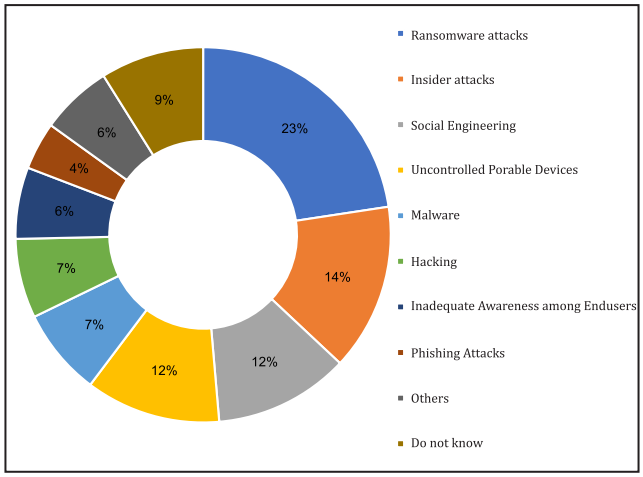
30% of the participant organisations stated that they have implemented the process which are being practised but they need to improve the process. 18% of the participant organisations stated that optimized process with respect to IT security.

According to the survey, majority (65%) of the participant organisations does not conduct information security audits on their vendors / business partners while 35% organisations carry out information security audits on their vendors / business partners.

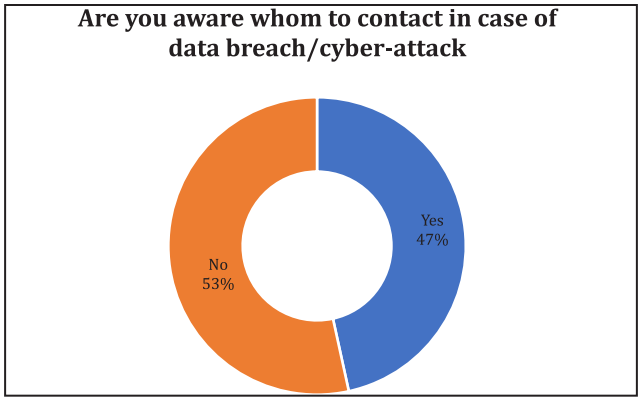
Does your organisation conduct security audits?



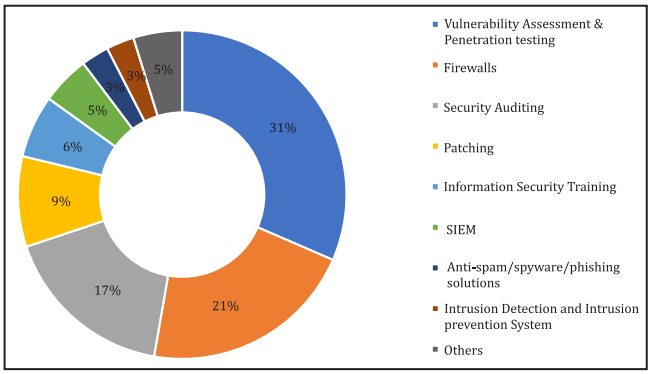
What do you consider the greatest security risk? According to the survey, 23% organisations considered ransomware attacks as the greatest security risk to the organisation, followed by social engineering (12%), insider attacks (14%), uncontrolled portable devices (12%).



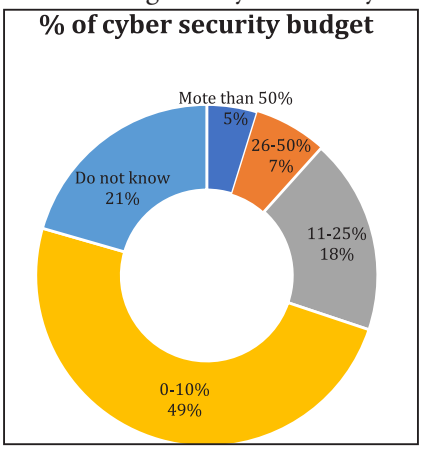
The survey revealed that 53% of the participant organisations are not even aware whom to contact in case they experience a data breach/ cyber-attack.



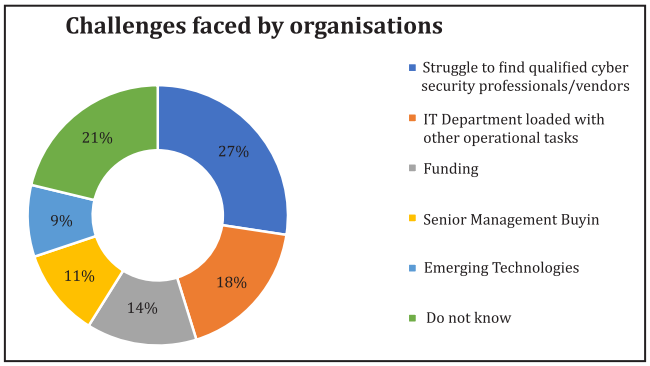
Which security measures have been implemented by your organisation? The survey revealed that 31% of the participant organisation have implemented Vulnerability Assessment & Penetration testing at their organisation, 21% have implemented firewalls at their organisations and 17% have implemented security audits at their organisations.



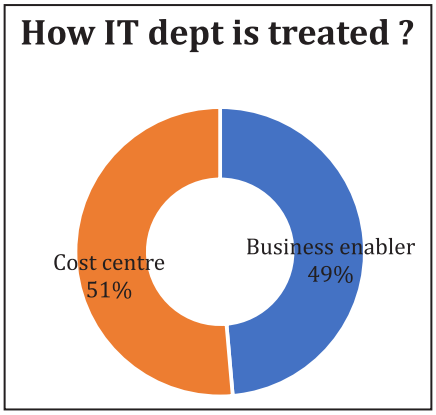
Only 5 percent of the participant organisations spent more than 50% of their IT budget on Cyber Security while 7% spent 26-50% of their IT budget on Cyber Security. It is noted that 49% of the organisation spent less than 10 percent of their IT budget on cyber security.



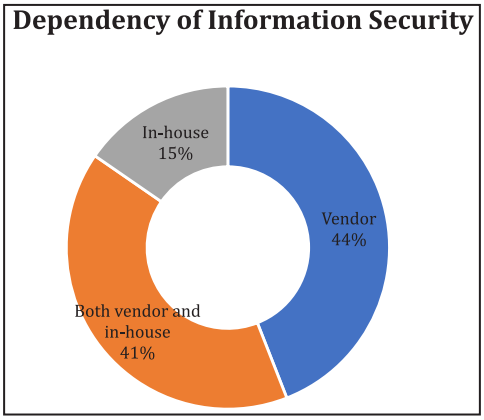
The survey identified that most of the organisation face challenges: to find qualified cyber security professional/ vendors (27%), IT department loaded with other operational tasks (18%) and other challenges such as lack of funds (14%), senior management buyin (11%) and emerging technologies (9%).



The survey stated that in 49% organisations, the cyber-security/IT department is treated as business enabler and only 51% organisations have treated them as cost centre.



According to the survey, 41% of the organisations utilise services of vendors along with in-house team for information security issues. Further, 44% organisations are only dependent on vendors.



Summary

The data of Cybersecurity Survey reveals that awareness level on cybersecurity in India Inc is increasing with some noted improvements over the few years. Especially there is a huge spike in cyber security in the corporate world in India. There has been increase in the number of cyber breaches in the recent past and so does the financial and reputational losses. Digitalisation and information exchange have increased over leaps and bounds so does the adoption of Technology. Technology being the enabler has an important part to play in our businesses be it corporate or personal.

Ransomware tops the charts as the greatest security risk to the organisation, followed by social engineering, insider attacks, uncontrolled portable devices. So it is quite evident that insider threat remains as industry's major problem in cyber security after ransomware.

There is huge demand for cyber security professionals as there is a shortage of skills and demand for finding qualified professional and vendors is on an all-time high. People are taking interest and seeking knowledge in this field, probably that's why India is the country with the highest number of security certifications.

One cannot deny that the government and top management including CEO's and board members have voted in favour of investing in Cyber Security Strategy be it technology adoption to improve surveillance, detection, prevention and incident response.

However, we still believe that cyber security is IT Security alone whereas IT forms just a part of bigger cyber security. Organisations need to work towards utilising and optimising their existing technology systems on cyber and aligning the same with an effective and implementable cyber security policy and procedure framework. Organisations need to combine people, process and technology for a more holistic approach towards security.

Majority of survey respondents have more than 25 people in IT teams but still it is noteworthy that 62 % of participating companies have suffered an cyber-attack in the form of ransomware, phishing or malware attack. Have bigger teams should not suffice but having a right mix of skilled and qualified resources and a partnership with right size vendors will serve the purpose.

The survey captures the need for conducting self-examination or diagnosis to review the technology and processes' to be prepared for any crisis situation. A Risk based approach is to form your data security strategy by prioritizing measures based on how much they will affect your bottom line. And to do this, your best tool is a thorough risk assessment.

It also puts an emphasis on conducting a mock drill exercise to put ourselves in an imaginary crisis situation just to examine our response to handle the crisis.

The survey results demonstrated that 30 % of the participant organisations does not have evidence of any systematic process with respect to IT security which is an area of concern. We should not only have a systematic process of IT Security, we should have processes, which well documented, well communicated and implemented and followed in the organisation towards making it an optimised process.

India is a country where crisis looms at large scale we should have an effective business continuity planning in place be it IT Disaster recovery or Functional Business Continuity in the case of manmade or artificial crisis like cyber warfare, terrorist attacks, riots, floods, Earthquakes or Fire Outbreak. It takes seconds for our business to get destructed, but it might take years and years to put together a successful business. The survey results demonstrate that a good amount of companies have the same in place, however, it should improve as business is volatile.

While audits can be carried out once or twice in a year due to other commitments the organisations carry employee awareness and training needs to be conducted more frequently as a low percentage of respondents are found to do that. As per the survey close to 60 % organisations does not have a formal process of educating their employees on a periodic basis. You don't need to breach a firewall or hack into your web applications if your employees can give out their credentials just because the attacker seemed to be more important, authoritative and skilled to create a fictitious situation to make him genuine or you start believing of what information he is seeking is right and he is the authorised recipient of the information.

Survey results say that 49% of the organisation spent less than 10 percent of their IT budget on cyber security. This should increase as cyber security should be viewed as an investment and not expense.

To sum it all there is always room for growth. Cybersecurity programs cannot advance alone. Indeed, barriers such as lack of cybersecurity awareness, skilful personnel and financial resources persist. Accordingly, organizations using cyber space need to take proactive steps by instilling positive change and making cybersecurity topmost priority. It is only then that we can move forward to avoid coming cyber-attacks.

Chapter

4

Cyber Security Breaches- The Dark Past

During beginning of 21st Century, internet access and use of computers was rapidly growing. The use of technology was increasing faster than the new security measures required. Such tremendous revolution of internet and computers also attracted huge amount of data breaches and cyberattacks. In these cyberattacks targeted confidential information of corporates as well as governments bodies. The key cyberattacks around the globe are:

Equifax (2017)

Cybercriminals penetrated Equifax (efx), one of the largest credit bureaus in July 2017 and stole the personal data of 145 million people. It was considered among the worst breaches of all time because of the amount of sensitive information exposed, including social security numbers.

Firms like Equifax, TransUnion and Experian sell that data to customers, such as banks, landlords and employers, so that they can learn more about you. Hence it could have an impact for years because the stolen data could be used for identity theft.

JP Morgan Chase data breach

In 2014, JP Morgan Chase data breach was a cyber-attack against American bank JP Morgan Chase that is believed to have compromised data associated with over 83 million accounts – 76 million households (approximately two out of three households in the country) and 7 million small businesses. The data breach is considered one of the most serious intrusions into an American corporation's information system and one of the largest data breaches in history.

Yahoo

In September 2016, the once dominant internet giant, while in negotiations to sell itself to Verizon, announced it had been the victim of the biggest data breach in history, likely by "a state-sponsored actor," in 2014. The attack compromised the real names, email addresses, dates of birth and telephone numbers of 500 million users. The company said the "vast majority" of the passwords involved had been hashed using the robust bcrypt algorithm.

A couple of months later, in December, it buried that earlier record with the disclosure that a breach in 2013, by a different group of hackers had compromised 1 billion accounts. Besides names, dates of birth, email addresses and passwords that were not as well protected as those involved in 2014, security questions and answers were also compromised. In October of 2017, yahoo revised that estimate, saying that, in fact, all 3 billion user accounts had been compromised.

The breaches knocked an estimated $350 million off yahoo's sale price. Verizon eventually paid $4.48 billion for yahoo's core internet business. The agreement called for the two companies to share regulatory and legal liabilities from the breaches. The sale did not include a reported

investment in alibaba group holding of $41.3 billion and an ownership interest in yahoo japan of $9.3 billion

Wannacry

Wannacry, which spanned more than 150 countries, leveraged some of the leaked NSA tools. In May, the ransomware targeted businesses running outdated windows software and locked down computer systems.

The hackers behind Wannacry demanded money to unlock files. More than 300,000 machines were hit across numerous industries, including health care and car companies.

Notpetya

In June, the computer virus Notpetya targeted Ukrainian businesses using compromised tax software. The malware spread to major global businesses, including Fedex, the British advertising agency WPP, the Russian oil and gas giant Rosneft, and the Danish shipping firm Maersk.

In September, Fedex attributed a $300 million loss to the attack. The company's subsidiary TNT express had to suspend business.

Bad Rabbit

Another major ransomware campaign, called bad rabbit, infiltrated computers by posing as an adobe flash installer on news and media websites that hackers had compromised. It scanned the network for shared folders with common names and attempted to steal user credentials.

The ransomware, which hit in October, mostly affected Russia, but experts saw infections in Ukraine, turkey and Germany.

Voter Records Exposed

In June, a security researcher discovered almost 200 million voter records exposed online after a GOP data firm misconfigured a security setting in its amazon cloud storage service.

Verizon and the US Department of Défense also had data exposed on amazon servers.

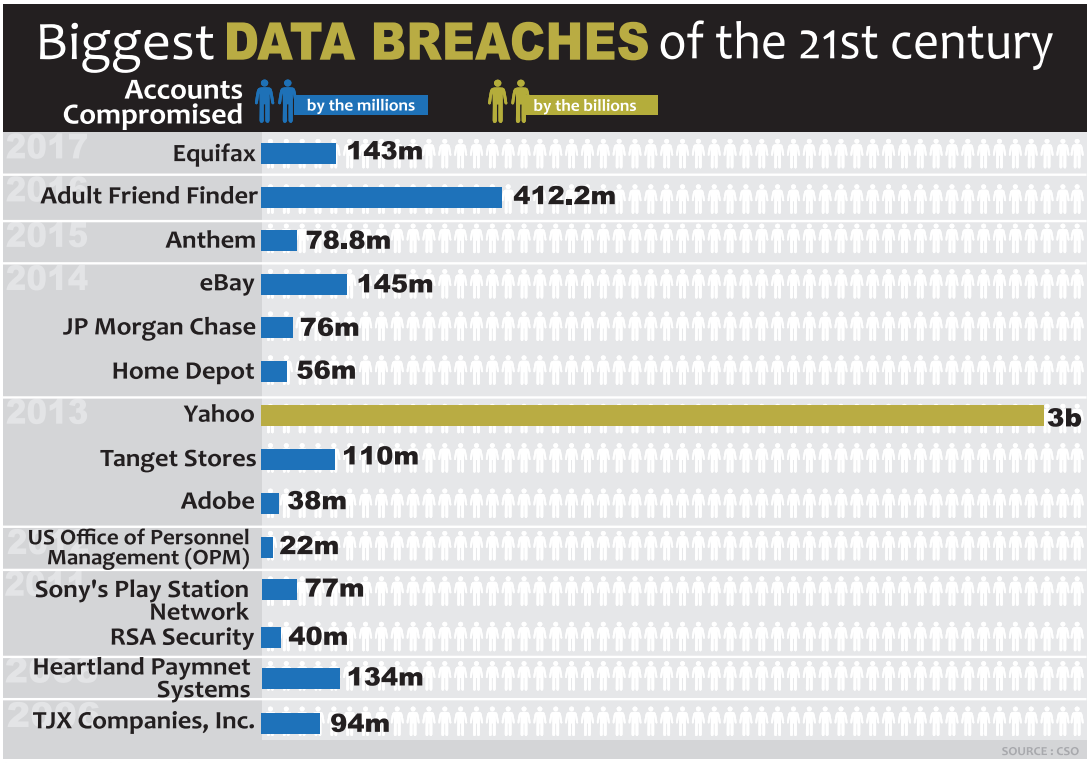
Hacks target school districts

The US Department of education warned teachers, parents, and k-12 education staff of a cyberthreat that targeted school districts across the country in October.

The group, dubbed the dark overlord, stole information on students, teachers and other district employees. They asked for money to destroy the files. Schools closed for three days.

An Uber coverup

In 2016, hackers stole the data of 57 million uber customers, and the company paid them $100,000 to cover it up. The breach wasn't made public until this November, when it



biggest data breaches by year and accounts compromised 1

was revealed by new Uber CEO Dara Khosrowshahi.

India Cyber Attacks

India is also not untouched from cybercrime. We are also facing continuous attacks of cyber criminals, hackers etc. and compromising private and confidential data. The key cyber attacks are:

Cosmos Bank Cyber Fraud: Pune, August 2018

Cyber criminals hacked the systems of India's cosmos bank and siphoned off a whopping INR 94.42 crore (approx. US$1.49 million) from the Pune-headquartered Cosmos Cooperative Bank Ltd - the second oldest and second biggest cooperative bank in India - to foreign and domestic bank accounts through simultaneous withdrawals across 28 countries over the weekend.

The co-operative bank said unidentified hackers stole customer information through a malware attack on its automated teller machine (atm) server, withdrawing 80.50 crore (approx. US$11.50 million) in 14,849 transactions in just over two hours on August 11, mainly overseas.

Besides, the ATM withdrawals, the hackers transferred INR 13.90 crore (approx. US$ 1.99 million) to a Hong-Kong based company's account by issuing three unauthorized transactions over the swift global payments network.

Indian Banks Data Breach, 2016

It was estimated 3.2 million debit cards were compromised. Major indian banks- SBI, HDFC bank, ICICI, yes bank and axis bank were among the worst hit.

2,500 twitter accounts linked to adult websites

Cybersecurity leader Symantec recently revealed that more than 2,500 twitter accounts have been compromised and are tweeting links to adult dating and sex websites. The attackers changed the profile photo and the basic information of the accounts to promote adult sites. The breach affected several high-profile accounts.

117 million Linkedin users exposed 3/ 6117 million Linkedin users exposed

Linkedin confirmed a breach that happened in 2012, which led to more than 100 million of its users' passwords being compromised. In an email sent out to all its members, linkedin admitted that the massive data breach in 2012 may result in millions of passwords being leaked to the internet. The data breach involved cyber theft of email addresses, hashed passwords and linkedin member ids (an internal identifier linkedin assigns to each member profile) from 2012.

IRCTC 'Hack'

India's largest e-commerce website IRCTC too came in the news recently when the reports surfaced of the website being hacked. Data of around 10 million customers was feared to have been stolen from the server of the e-ticketing portal.

Flipkart CEO Binny Bansal's email 'Hack'

CEO of India's biggest e-commerce website Flipkart Binny Bansal's official email account was hacked, and two mails were sent from it to the company's CFO asking to transfer $80,000. It was later found that the account was not hacked but spoofed.

Swift tech lapse

The theft of US$81 million from the Bangladesh's central bank found that the international banking payments network swift committed several mistakes in connecting a local network, which led to the hack and since then investigators are said to have identified breaches at as many as 12 other banks.

Detailed Overview on Dark Past-Case Studies

Wanna cry attack

What was happened?	What helped make this attack successful?
• It was a cyber-attack conducted on a large scale, targeting only the Microsoft Windows operating systems. • The initial infection was likely through an exposed vulnerable SMB port, and then email phishing was the main method of spreading the WannaCry ransomware. • In this attack, the ransomware would encrypt all the files in your computer. To remove such encryption, one was asked to pay approximately $300 worth in bitcoins, with a deadline.	• The main victims of such cybercrime were Windows 8, 2003 and XP users, because the last released security update for XP was in April 2014, and many didn't install the newer update as of March this year. • Microsoft had stopped supporting these versions of windows, but an emergency update was released for them to fight this cyber-attack. • Also, there were many using an unlicensed windows software, and attack had exploited a vulnerability in Windows OS called Eternal Blue.

Impact	**The Cure**
• This attack impacted several businesses, institutions and hospitals all over the world. • Businesses like Nissan and Renault had to pause their activities after some of their computers were affected. • Estimates state that around 200,000 to 300,000 computer systems were affected in this attack in approximately 150 countries.	• While trying to establish the size of the attack, a man named Marcus Hutchins accidentally discovered a "kill switch" coded in the malware. He registered a domain name for the DNS sinkhole (a DNS which gives false information about a domain), which stopped the spreading of the virus like a worm, thus drastically slowing down the spread of the virus, giving time to come up with defensive measures. • A man named Adrian Guinet created a "WannaKey", a solution to the WannaCry ransomware based on its flaws. He cautioned that it wouldn't work if the infected computer was rebooted or if the malware overwrote the decryption key.
Future learnings	
• Always use latest version device/software. • Get your systems/devices patched with latest updates/ upgradations. • Always have backup/copy of your data, isolated from your working network and physical environment. • Never open/click any link/script/file coming from an unknown/untrusty source.	

Cosmos Bank's online fraud

What was happened?	**What helped make this attack successful?**
• Pune-based Cosmos Bank lost Rs 94 crore in a coordinated digital fraud comprising thousands of online transactions, made possible because of a malware attack on the bank's systems.	• This attack was performed using a malware which compromised the digital system responsible for settling cash dispensation requests raised at ATMs. The hackers exploited malware vulnerability in its automated teller machine (ATM) switch system. • As soon as one swipes a card, a request is transferred to the core banking system (CBS) of the bank. If the account has enough money, the CBS will allow the transaction.
The Impact	**Future learnings**
• In this case, the malware created a proxy system that bypassed the CBS and approved a series 14,800 fraudulent transactions to withdraw Rs 80.5 crore — Rs 78 crore through 12,000 transactions in 28 countries, the rest in India. • Another Rs 13.5 crore was transferred to a Hong Kong-based entity using a facility called Society for Worldwide Interbank Telecommunications (SWIFT). • SWIFT is a network that enables financial institutions to send and receive information about transactions in a secure environment.	• All banks need to upgrade their security mechanisms. • Banks should ensure that their systems are patched immediately after the update. • The RBI has clear guidelines and if these are followed, such incidents will not happen. • Bank/companies need to understand the kind of exploits being used and then neutralise them and should develop future attack prevention strategies.

Equifax: Data breach costs estimated $439m.

What was happened?

- Equifax, one of the three major consumer credit reporting agencies, faced an attack in which hackers had gained access to company data that potentially compromised sensitive information for 143 million American consumers, including Social Security numbers and driver's license numbers.
- Equifax, based in Atlanta, is a particularly tempting target for hackers. If identity thieves wanted to hit one place to grab all the data needed to do the most damage, they would go straight to one of the three major credit reporting agencies.
- If you have a credit report, chances are you may be in this breach. The chances are much better than 50 percent.

What helped make this attack successful?

- Criminals gained access to certain files in the company's system from mid-May to July by exploiting a weak point in website software, the tool is called Apache Struts, and it's used by many large businesses and government organizations. Equifax used it to support its online dispute portal -- where Equifax (EFX) customers go to log issues with their credit reports. The flaw allowed hackers to take control of a website.
- This vulnerability was disclosed back in March. There were clear and simple instructions of how to remedy the situation. The fact that Equifax was subsequently attacked in May means that Equifax did not follow that advice.

Impact

- In addition to the other material, hackers were also able to retrieve names, birth dates and addresses. Credit card numbers for 209,000 consumers were stolen, while documents with personal information used in disputes for 182,000 people were also taken.

Future learnings

- Companies need to follow scheduled audits/pen testing's in respect of configurations and privileges decided.
- Many times, data exposure happens due to carelessness and unawareness of people so, Time to time awareness for the clients/customers and cyber security training is an essential weapon of data exposure war.

Cryptojacking: Over 2,000 computers at Aditya Birla Group held hostage by hackers' mining cryptos

What was happened?

- India suffered the first big 'cryptojacking' attack April 2018. The target was the Aditya Birla NSE 0.70 % Group — one of the country's largest business conglomerates headquartered in Mumbai.
- More than 2,000 computers of various companies of the group were targeted by hackers for cryptojacking — a new kind of cyber-warfare where hackers misuse a target's terminals and their processing power to mine crypto currency.
- "It's a kind of attack where the primary intention of the hackers is not to steal information and cause business disruption. Rather, they hijack the target's computers and tap the power supply to the organisation to mine crypto coins, which requires a lot of energy.
- In this attack, the cryptocurrency mined was Monero, an open-source cryptocurrency that focuses on privacy and is virtually untraceable.

What helped make this attack successful?

- Cryptojacking is the infiltration of malware to enable browser-based mining of cryptocurrencies on infected websites.
- The attack was first detected about a month ago at one of the group's overseas subsidiaries. Within days, the malware found its way into some of the group's manufacturing and other services companies.

Impact	**The cure**
• Cryptojacking affects anything that runs a browser with JavaScript. So, your desktop, laptop and even your mobile phone could be potential targets.	• First, let be very clear, it's Not Easily Detectable. Apart from power usage, cryptojacking doesn't directly cause any harm to victims. "Affected users will notice their device slowing down due to the high CPU usage in addition to higher electricity bills. This process also generates a lot of heat, and we've seen physical damage of devices.
Future learnings	
• Among the key mitigaation steps that can be taken are: using browser extensions that block mining scripts, adopting the browser isolation model and carefully monitoring endpoint devices' use of resources. • In a browser-based cryptojacking, a cryptocurrency mining code is embedded into a website, and site visitors run the mining code via their browser. So, companies need to regularly review scripts run on their systems.	

BGP hijacking attacks

What was happened?	**What helped make this attack successful?**
• Malicious actors redirected a portion of internet traffic flowing across Amazon Web Services (AWS) for approximately two hours before stealing around $150,000 in cryptocurrency from MyEtherWallet.com virtual wallets.	• The attack used a hacking technique where internet traffic is intercepted from a legitimate website and redirected to a fake website (in this case one for MyEtherWallet.com). This allowed the attackers to steal customers' legitimate logon details to empty their cryptocurrency wallets. • The attack hijacked the Border Gateway Protocol (BGP), a key protocol used for routing internet traffic around the world. The security of the internet depends on routing security. However, security was never built into BGP, which is decades old.
Impact	**Future learnings**
• According to ISOC, in 2017 alone there were 14,000 routing outages or incidents which led to stolen data, lost revenue, reputational damage and more. ISOC states that MANRS will address these threats through technical and collaborative action across the internet.	• Widespread effective management of routing protocols by IXPs and CPS would minimise the most common routing threats to internet traffic and would have reduced the impact of the BGP hijack experienced by MyEtherWallet.com • MANRS (Mutually Agreed Norms for Routing Security) should be adopted by internet exchange points (IXPs) and Internet Service Providers (ISPs) who control international internet connectivity.

Chapter 5

Cyber Security—The Legal Framework

For more than a decade, cyber security has been a concern for the government and private sector alike. The growth in information technology and e-commerce sector have given rise to cyber-crimes, causing a huge loss to the government and its people across the globe.

Data breaches have gained more attention due to the impact of digitization on financial, healthcare, SMEs and other industries. Even though data breaches occurred way before digitization took the world by storm, but the popularity of the digital platforms gave a new dimension to these breaches as the importance, volume, and cost of the data breaches have increased considerably.

Cyber security regulations play an important role in laying a strong enforcement mechanism with the virtue of which companies and organizations to protect their systems and information from cyber-attacks such as viruses, trojan horses, phishing, denial of service (dos) attacks, unauthorized access (stealing intellectual property or confidential information) and control system attacks.

To combat with cybercrime and protect data from cyber criminals, governments of many countries including india have implemented robust law and regulations. The outline of various international and local laws and regulations which govern the cyber security landscape are below.

How the Law Around Globe

US-Federal Laws

The federal government of USA, implemented three main federal cybersecurity regulations –

- Health insurance portability and accountability act (hipaa), 1996
- Gramm-leach-bliley act, 1999
- Homeland security act, 2002 which included the federal information security management act (fisma)

These three regulations mandate that healthcare organizations, financial institutions, and federal agencies should protect their systems and information. However, these rules are not foolproof in securing the data and require only a "reasonable" level of security.

Other Regulations

In a recent effort to strengthen its cyber security laws, the federal government is introducing several new cyber security laws as well as amending the older ones for a better security ecosystem. Below are a few of them:

Cybersecurity information sharing act (CISA) – its objective is to improve cybersecurity in the united states through enhanced sharing of information about cybersecurity threats, and for other purposes. The law allows the sharing of internet traffic information between the U.S. Government and technology and manufacturing

companies. The bill was introduced in the U.S. Senate on July 10, 2014, and passed in the senate October 27, 2015

Cybersecurity enhancement act of 2014: it was signed into law December 18, 2014. It provides an ongoing, voluntary public-private partnership to improve cybersecurity and strengthen cybersecurity research and development, workforce development and education and public awareness and preparedness.

Federal exchange data breach notification act of 2015: this bill requires a health insurance exchange to notify each individual whose personal information is known to have been acquired or accessed as a result of a breach of security of any system maintained by the exchange as soon as possible but not later than 60 days after discovery of the breach.

National cybersecurity protection advancement act of 2015: this law amends the homeland security act of 2002 to allow the department of homeland security's (dhs's) national cyber security and communications integration center (nccic) to include tribal governments, information sharing, and analysis centers, and private entities among its non-federal representatives.

European Union-General Data Protection Regulation (GDPR)

The General Data Protection Rregulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

Key regulations in GDPR are as:

- **Breach Notification:** Under the gdpr, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.
- **Right to access :** Part of the expanded rights of data subjects outlined by the gdpr is the right for data subjects to obtain from the data controller confirmation as to whether personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.
- **Right to be forgotten** also known as data erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.
- **Data portability**

  GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine-readable format' and have the right to transmit that data to another controller.
- **Privacy by design**

  privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the gdpr. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - 'the controller shall. Implement appropriate technical and organizational measures. In an effective way. To meet the requirements of this regulation and protect the rights of data subjects'.

Data Protection Officers

Currently, controllers are required to notify their data processing activities with local dpas, which, for multinationals, can be a bureaucratic nightmare with most member states having different notification requirements. Under gdpr it will not be necessary to submit notifications / registrations to each local dpa of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the model contract clauses (mccs). Instead, there will be internal record keeping requirements, as further explained below, and dpo appointment will be mandatory only for those controllers and processors whose

core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:

- Must be appointed based on professional qualities and expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant dpa
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could results in a conflict of interest

Superseding the data protection directive 95/46/ec, the regulation contains provisions and requirements pertaining to the processing of personally identifiable information of individuals (formally called data subjects in the GDPR) inside the EU, and applies to all enterprises, regardless of location, that are doing business with the EEA.

Penalties

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or€20 million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. Not having enough customer consent to process data or violating the core of privacy by design concepts. There is a tiered approach to fines e.g. A company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

Cyber Law – Indian Context

Cybercrimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian penal code. In India, breach of content of messages, calls etc. was protected by Indian Telegraph Act, 1885. In the emerging technologies, immense use of internet and the abuse of computers have also given birth to a gamut of new age crimes in end of 20th century. The Indian government addressed these issued by the information technology act, 2000.

Quick Quide - Cyber Laws in India

Information technology act, 2000 (amendment 2008) is India's mother legislation regulating the use of computers, computer systems and computer networks as also data and information in the electronic format. This legislation has touched varied aspects pertaining to electronic authentication, digital (electronic) signatures, cybercrimes and liability of network service providers.

Sr. No	Offences	Section under it act
1.	Tampering with computer source documents	Sec.65
2.	Hacking with computer systems, data alteration	Sec.66
3.	Sending offensive messages through communication services, etc.	Sec.66a
4.	Dishonestly receiving stolen computer resource or communication device	Sec.66b
5.	Identity theft	Sec.66c
6.	Cheating by personation by using computer resource	Sec.66d
7.	Violation of privacy	Sec.66e
8.	Cyber terrorism	Sec.66f
9.	Publishing or transmitting obscene material in electronic form	Sec.67
10.	Publishing or transmitting of material containing sexually explicit act, etc. in electronic form	Sec.67a
11.	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form	Sec.67b
12.	Powers to issue directions for interception or monitoring or decryption of any information through any computer resource	Sec.69

13.	Power to issue directions for blocking for public access of any information through any computer resource	Sec.69a
14.	Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security	Sec.69b
15.	Unauthorised access to protected system	Sec.70
16.	Penalty for misrepresentation	Sec.71
17.	Breach of confidentiality and privacy	Sec.72
18.	Publishing false digital signature certificate	Sec.73
19.	Publication for fraudulent purpose	Sec.74
20.	Act to apply for offence or contraventions committed outside india	Sec.75
21.	Compensation, penalties or confiscation not to interfere with other punishment	Sec.77
22.	Compounding of offences	Sec.77a
23.	Offences with three years' imprisonment to be cognizable	Sec.77b
24.	Exemption from liability of intermediary in certain cases	Sec.79
25.	Punishment for abetment of offences	Sec.84b
26.	Punishment for attempt to commit offences	Sec.84c
27.	Offences by companies	Sec.85
Note: sec.78 of IT Act empowers police inspector to investigate cases falling under this act		
28.	Sending threatening messages by e-mail	Sec.503ipc
29.	Word, gesture or act intended to insult the modesty of a woman	Sec.509ipc
30.	Sending defamatory messages by e-mail	Sec.499ipc
31.	Bogus websites, cyber frauds	Sec.420ipc
32.	E-mail spoofing	Sec.463ipc
33.	Making a false document	Sec.464ipc
34.	Forgery for purpose of cheating	Sec.468ipc
35.	Forgery for purpose of harming reputation	Sec.469ipc

"Cyber Security is the term used to protect overall information systems and data residing on the same from any cyber threats and ensures dependent operational resilience.

I feel with respect to cyber security preparedness in India there is a positive trend in terms of cyber preparedness especially in critical infrastructure and highly regulated environment but long way to go. Honestly it is a catch up game and in today's digital world where hacking tools are easily available in the dark web and computing resources available at a cheaper cost. Organizations has to gear up to cope with the cyber trends . Some Basic hygiene measures which we should adopt to make India Inc cyber safe include Patching , Deploying Quick Detection Capabilities and Response and Measuring your cyber exposure in business and operational terms.

– Mr. Makesh Chandramohan
Chief Information Security Officer
Aditya Birla Capital Limited

Chapter

Chapter 6

Ever Changing Digital World

(How the change in technology is impacting cybersecurity)

Cybersecurity professionals are accustomed to securing access to their networks and applications. But digital transformation leads to an explosion of connected environments where perimeter protection is no longer enough. Attackers and other malicious individuals will continue to compromise weak links, resulting in deep access to companies' networks, systems, and data.

In a digital world, the classic, contained enterprise network no longer exists. For that reason, security must be embedded into all applications as the first line of defense, to achieve that level of security, we need to focus on "security by default" approach, in which an application's embedded security controls are, by default, set at the highest levels of protection. "The idea is to build in security, rather than asking users to opt in," he says. That's one of the hallmarks of being more proactive in securing data: protection is the default posture.

"self-defending apps" are another example of proactive security. This active-protection technique provides applications with advanced access-control capabilities, allowing them to react to malicious source-code modifications and debugging at runtime.

Cyber Security is the process of protecting computers, data and various kinds of programs from illegitimate access or attacks which are done with an aim of exploitation or misuse.

We look at how technology has affected cyber security-

Insider Threat

Among the most important factors for heading off insider threats are two-factor authentication (which verifies a user's identity via two different methods) and role-based access controls (which limit the user's access to data by job role). "The insider threat is very real. There are a lot of data breaches today by people who have a legitimate authorization that is too broad. They get to see more than they are entitled to. Two-factor authentication dramatically increases the security of the communications."

- **Security Breaches:** These types of crimes occur when the intruder tries to take advantage of employees using various types of scams. With the rise in technology and information available at the click of a finger, it is becoming easier for cyber criminals to gain access and use it to defame and misuse important data. Hackers do this is by scams and finding loopholes in corporate security systems.
- **Social Media Breaches:** These are one of the most common and easily accessible breaches. With social media becoming a by-default part of our lives it is becoming child's play for intruders to find out your personal information and use it for unfair means. Some of the examples are password stealing, hacking, bulk messages, fraudulent reviews and stealing of bank account information. They also involve social spam.

It can occur on any website or social media network.

- **Digitization:** Today companies worldwide are increasingly using cloud computing. Not only it saves time but also your money and resources. The process involves storing important data and at times very confidential information. Cloud Computing is an extremely methodical and profitable way of getting work done for the organizations. But very easy for hackers to gain information through the very process of cloud computing.
- **Botnets:** They were used in earlier stages of technological advancement. The process involved setting up a number of computers to forward information such as spams and messages. However now with the emergence of technology hackers are sparing no effort in taking this one step ahead and using botnets to collect more sensitive data such as name, address, financial information, other online activity.
- **Malware:** Hackers use malware to directly attack your computer to find out data. It consists of viruses, Trojan horses, and computer worms. The typical ways in which malware affect your computers are where you open an email attachment. It can also occur by downloading infected files during file sharing. Also always look for HTTPS protocol in your browser bar and not the only HTTP. Here the S stands for secure.
- **Spammers:** Spams are malicious bulk messages which are sent through email, instant messaging or other communication tools. They are normally used by advertisers since there are almost zero operational a costs involved.
- **Spear Phishing:** It is more serious than normal phishing emails. Regular phishing emails normally target random people but spear phishing involves accessing information for monetary gains, finding out business relevant information. Due to the advanced technology, there are even different ways to prevent from Phishing attack.
- **Identity Thefts:** Identity spoofing is also a matter of great concern in which the victim is bluffed. This happens normally on social networking sites.It may involve more deep crimes such as meddling with the IP address or stealing credit card information.
- **MIM Attacks:** It stands for Man-in-the-Middle attack. It is a kind of an ambush in which the intruder secretly impedes messages or data between two people or groups in conversation with each other. It is a highly dangerous form of attack; you can literally say it is kind of keeping tabs on your each and every word of communication. E.g.-online banking and e-commerce websites are common examples.
- **Smart Grids and Meters:** With the huge leap of technology and state-of-the-art electronic meters, consumers benefit from the proper usage of electricity. It also ensures proper distribution of electricity. However, not everything is as rosy as it seems. Information theft is very easily possible and cyber criminals will easily find ways to crack smart grids and steal the information.
- **Cloud Technology:** The cloud is set to have a significant impact on the transformation of systems security technology. More business enterprises and government agencies have embraced cloud technology to store the vast amounts of information that they generate on a daily basis.

There will be more approaches to information systems security that will be developed for use in the cloud. Techniques for on-premise data storage will be migrated to the cloud. Components such as virtualized intrusion detection and prevention systems, virtualized firewalls and virtualized systems security will now be used from the cloud as opposed to the traditional forms.

For instance, both private and public entities have doubled up their data center security by the use of IaaS services, such as Firehost and Amazon. Another perfect example of certified secure enough services that are based on the cloud is the GSA FedRAMP, which makes it easier for the small- to medium-sized business enterprises to have a data security center that is above average.

So, what is the solution for this?

We obviously cannot give in to these cyber criminals since technology will keep on advancing with each passing day. While the common solutions include staying alerted at all times you should also educate yourself with basic knowledge of not letting spam message erode your computer.

Chapter 7

Are We Aware Enough?

(How much Indian Corporate and people are aware about cybercrime and security)

In India each minute one person become internet users. its convergence with digitally supported platforms and gadgets, safeguarding the corporate as well as govt sector from the cybercrimes is becoming a challenging task. In addition to, the pinching reality is that the internet users are not getting updated on the vulnerable cyber threats and security issues, at the pace they are getting updated with the usage of internet enabled tools and apps.

Usage of Internet has become a daily routine for majority of people for day-to-day transactions. It is not just the technology of Internet that is luring the users, but the convergence of Internet with various digitally supported platforms and services that make the users hook to it like never before. We abundantly depend on internet provided information quite often either for office chores, e-commerce, banking, weather forecasts, business deals, fitness tips, share markets, entertainment, fun, satisfying psychological urges and emotions, and passtime activity etc.

Upload, share, download, Google it, Apps etc., are treated to be quite common jargons these days that are functioned at finger tips. Hence, it is no exaggeration to say that smart phones and other internet enabled personal electronic gadgets has entered every realm of life and opened gates for cybercrimes to flood in.

Lack of awareness on such issues would end up in a severe damage on financial, emotional, moral, or ethical grounds. Under such dire scenario, besides tackling the cybercrimes, another issue that needs to be focused on higher priority is – creating awareness on "cybercrimes and security" among the internet users. Thus the current study focuses in finding out the answers to alarming questions – "Are people really aware that he/she is vulnerable to various cyber-crimes?"; "If people are aware, to what extent?", "If not aware of cybercrimes, what measures can be adopted to

User's awareness in this particular context can be referred to the level of attention and knowledge that enables the internet users to understand what an Internet is; how it works; its environment and functionalities; do's and don'ts of internet; uses, misuses, its consequences; transactions through internet; vulnerable threats and remedial functions; including other users and governance factors such as laws and regulations. These parameters would enable to predict the levels of awareness and understanding towards cybercrimes and security.

The study also tried to analyse how the internet users perceive the overall issue of cybercrime and what exactly it is for them. Criminals are taking advantage of the fast internet speed and convenience provided by the internet to

perform large and different criminal activities, says Agarwal (2015). In her paper, she insisted that it becomes the duty of all the internet users to be aware of the cyber-crime and the cyber law made to deal with cyber-crimes. She has also discussed the types of cyber-crime, which can help users to identify the crime that they have been victim of.

The experts opined that internet users still lack knowledge and awareness on cybercrimes, pan India. The challenges that cybercriminals are becoming tougher day by day and the government must keep a vigilant eye on the happenings. 'Unfortunately, there is a huge dearth of cyber experts to handle the issues when compared to number of cases that are being filed in India"

83% respondents use internet on smart phones quite regularly. 15% people sometimes use internet on smart phones and 2% occasionally.

- Most of the respondents (83%) have their own laptop or PC. 17% people don't have laptop or computer.
- Most of the respondents (75%) have replied that more than one person uses Internet at home, mostly the siblings. 45% opined that their parents know how to use Internet.
- 95% people use internet daily basis and 2.5 % people use internet in weekly twice and 2.5% people use internet rarely like once in a month.
- 43% people spend their 3 to 5 hours on internet. 37 % people spend 1 to 2 hours of time on internet. 8 % people spend their 6 to 8 hours and 12 % people spend 9 hours or above.

Regarding awareness on various types of cybercrimes 64.4% people know about Awareness on other kinds like cyber stalking, Phishing, Identity theft, Cyber Bullying, Tor and deep web crime, mobile hacking, Child soliciting and abuse etc is less. levels did not cross 9% for any of these serious issues.

- 79% of respondents know that downloading from illegal torrents and blocked URL is a
- 21% of respondents don't know that downloading from illegal torrents and blocked URL is a
- 56% of people know that accessing block torrents ends you up in jail for 3 years and fine of 3 lakhs of rupees.
- 12% of respondents have heard about cybercrimes from the known people / people of proximity who have personally experienced
- 68% of respondents have not heard about 'Cyber Cells" and literally don't know reporting the cybercrime, other than approaching police. Section –III- Awareness on Cybercrime & Security
- Only 15% have referred to IT Act. that IT act deals with cybercrimes, but never referred it or read it. 24% IT Act, but not sure that cybercrimes are covered under it. Remaining 18% have no idea about IT Act at all (Refer to Figure 1) Figure 1: Awareness on IT Act Among Internet Users), ISSN: 2456-6470 13 Regarding awareness on various types of cybercrimes 64.4% people know about Hacking.

Awareness on other kinds like cyber stalking, Phishing, Identity theft, Cyber Bullying, Tor and deep web crime, mobile hacking, Child soliciting and abuse etc is absolutely less. The awareness for any of these serious % of respondents know that downloading from illegal torrents and blocked URL is a crime. 21% of respondents don't know that downloading from illegal torrents and blocked URL is a crime. 56% of people know that accessing block torrents for 3 years and fine of 3 lakhs of 12% of respondents have heard about cybercrimes from the known people / people of proximity who have personally experienced it.

The study proves that internet users are not thoroughly aware of cybercrimes and cyber security that are prevailing. A growing net addiction is visible in towns. The convergence of smart phones and internet are on stride and quite popular.

This means, there is more scope for cybercrimes. Though many internet users claim to be aware of such crimes, still majority consider the cybercrime as hi-fi politically motivated attacks on big organizations. A significant amount of internet users are not even aware whom to contact or report for any grievances regarding cybercrimes.

The lack of awareness is also observed drastically in case of protection towards their personal PCs and laptops also, as half of the respondents are still the victims of various virus, not been updating their passwords from time to time, and have the tendency of sharing their personal information with others. Regarding the illegal downloads, though the internet users are aware of consequences, still they take this activity for granted and been downloading movies, games and music easily from various torrents. Ignorance on this issue can grow further if the government fails to take serious attempts in implementing the rules and regulations in this regard.

As the dotted red line indicates, the Govt. can take initiative of creating awareness among people and stakeholders at various levels, with multiple approaches, like

❖ Inform and educate all the stakeholders on cybercrimes and security measures as they deal with public on a larger scale through internet. For instance, the bank can take the responsibility to alert the customer through personal counselling or by providing information whenever required.

❖ Encouraging cross-flow of knowledge and information between media, cyber cells, ethical hackers and education sectors to reach the people in easiest and appropriate way.

Protection for cybercrime does not merely entail creating institutional mechanism and agencies equipped with the latest forensic and investigation tools. As it also depends on the ability of the end user to safeguard himself against malicious online content, for which the governments have launched programs to increase public awareness.

These are some areas on which most of the governments are focusing.

1. **Government body cybersecurity accountability:** Dedicated ministry accountable for devising a national strategy and fostering local, national and global cross-sector cooperation.
2. **National cybersecurity coordinator:** Department or individual who oversees cybersecurity activities across the country.
3. **National cybersecurity center point:** A multi-agency center, which serves as a focal point for all cyberspace threat activity.
4. **Legal measures:** Review of cyber laws and, if necessary, amend the existing law, create new procedures, and policy to deter, respond to and prosecute cybercrime.
5. **Cybersecurity framework:** Framework with minimum or mandatory security requirements on issues, such as risk management and compliance
6. **Cybercrime reporting and analysis:** Analysis of cyber threat trends, coordinates response and disseminates information to all relevant stakeholders.
7. **Cybersecurity awareness and education:** A national program to raise awareness about cyber threats on a continuous basis.
8. **International cooperation:** Global cooperation is vital due to the transnational nature of cyber threats.

"Cyber Security has become an integral part of corporates & it's now no more a topic of Information Technology but it's a Topic of Board now. We have to see Cyber Security completely different then Information Security, todays Cyber Security is more to do with defending your organization from sophisticated new age targeted attacks with the help of cutting edge tools & technologies rather than only focusing on policies & procedures. India Inc. is getting prepared from sophisticated cyber-attacks thankfully from the push from Govt & respective regulators which are ensuring that the boards should take interest in cyber security so we are now moving in right directions to become mature in Cyber Security. we should think about proactive cyber defense as our main strategy to become cyber resilient which includes investing in cyber security tools & technologies, adapting new processes & nurturing talents in cyber security."

– Amit Ghodekar

Vice President | Information Security

Motilal Oswal Financial Services Limited

"Organization should think about data protection & cyber security right in the beginning of selecting their tech stack to optimize their spending on Cyber security infrastructure. Open source is promising area where we should look for securing data. Another important approach is close all Gates and reduce risk, instead of keep everything open in your IT infrastructure and spend lot of money and energy in trying to secure it."

– Mr. Dhammapal Chawhan A

Assistant Managing Director

Haryana State Electronics Development Corporation Limited (Hartron)

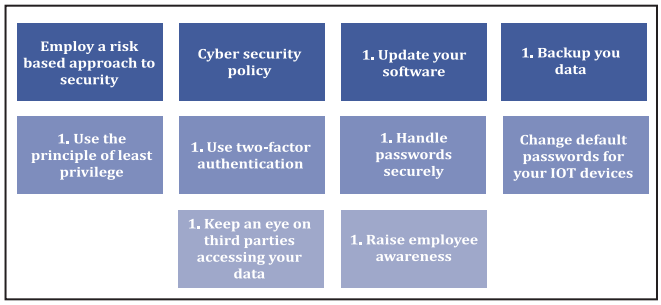
Chapter

8

How to Combat- The Best Practices

The fact cannot be denied that cyber-crime is still growing, and still is an unidentified threat to the employees constantly.

There are various preventive measures are available to combat with cybercrimes and attack. The key measures are:



1. **Employ a risk-based approach to security:** A risk-based approach is to form your data security strategy by prioritizing measures based on how much they will affect your bottom line. And to do this, your best tool is a thorough risk assessment.

   Here's what a risk assessment allows you to do:

   - Identify all valuable assets, including those you were not aware off
   - Identify the current state of cyber security in your company
   - Identify the most pressing threats your data faces and how those threats may affect your bottom line

2. **Form a hierarchical cyber security policy:** First, a written policy serves as a centralized, formal guide to all best practices for cybersecurity as well as all security measures used in your company. It also allows you to make sure that your security specialists and employees are on the same page and gives you a way to enforce rules that protect your data. However, the workflow of each department can be unique and can easily be affected by needless cyber security measures.
3. **Update your software:** Why are software updates so important? The main reason is because the majority of malware out there doesn't exactly target new and unknown security vulnerabilities. Instead, it goes for well-known exploits that have already been fixed in the latest versions in the hopes that companies haven't updated.

   So, what keeps companies using old software? There are several reasons:

   - Removed or altered functionality in newer versions may force staff to relearn or readjust established processes.
   - Update processes may be too complex and may disrupt existing workflows.

- ❖ Updates may be too costly or even unavailable, forcing a company to switch to a more modern solution.

4. **Backup your data:** Data backup is another basic security measure that has gained increased relevance in recent years. With the advent of ransomware – malicious software designed to encrypt all your data and block access to it until you pay a hefty sum for a decryption key – having a full current backup of all your data can be a lifesaver.

   You need to make sure that your backups are thoroughly protected and encrypted and that they are very frequently updated. It's also best to divide backup duty among several people to avoid insider threats.

5. **Use the principle of least privilege:** Many companies, particularly smaller ones, tend to grant new employees all privileges by default. This allows employees to access sensitive data even if they don't necessarily need to. Such an approach not only poses an additional risk in terms of insider threats, but also allows external hackers to get access to sensitive data as soon as any of your employee accounts is compromised.

   Best approach is to use the principle of least privilege, in other words to assign each new account the fewest privileges possible and to escalate privileges as necessary. At the same time, when access to sensitive data is no longer needed, all corresponding privileges should be immediately revoked.

6. **Use two-factor authentication:** Two-factor authentication is an important security standard when it comes to account protection. It employs an additional physical device, such as a security token or a mobile device, to confirm the identity of the person behind the screen. This authentication method provides a very reliable login procedure if the secondary device doesn't get lost or stolen. As an added benefit, it also allows you to clearly distinguish among users of shared accounts, making access control easier.

   Two-factor authentication is so effective that the fbi even promoted it as part of national cyber security awareness month.

7. **Handle passwords securely:** The first thing you need to know is that passwords need to be long, complex, and fully unique.

   Here are the main things you should consider regarding password handling:

   - ❖ It's better to use a longer, easy-to-remember phrase as a password than a short string of random characters.
   - ❖ Each password needs to be fully unique – make sure to prohibit your employees from using their passwords on other accounts.
   - ❖ Prohibit your employees from sharing credentials with each other. While it may be more convenient for them, it is extremely unsafe.

8. **Change default passwords for your IOT devices:** Many internet-enabled devices come with a set of default credentials hard-coded inside. Such credentials are usually freely available on the internet and widely known to perpetrators. Most malware targeting iot devices looks for devices that keep using their default credentials to hijack them and add them to an army of bots that are ready to conduct massive denial of service attacks at the push of the button.

   What can you do about this? The only way to make sure that your devices are protected from being infected is to change all default credentials as soon as possible. Make sure that your new passwords are fully unique and complex.

9. **Keep an eye on third parties accessing your data:** Nowadays, almost every company has a network of third parties working with it remotely. Third-party access not only provides a greater risk of insider attacks, but also opens the way for malware and malicious hackers to enter your system.

   The best way to protect your sensitive data from any breaches via third-party access is to use temporary passwords. Temporary passwords allow you to limit the scope of access that third-party users have and allow you to make sure that you know who exactly connects to your network and why.

10. **Raise employee awareness:** It's hard to believe, but the key to protecting your data lies with your employees just as much as with your defences.

    The best way to deal with negligence and security mistakes by your employees is to educate them on why security matters.

    Make sure your employees know why certain measure are in place and why they're important. It's much better to get your employees the proper training than to deal with a data breach caused by accidental actions.

6 Critical Steps for responding to a cyber attack

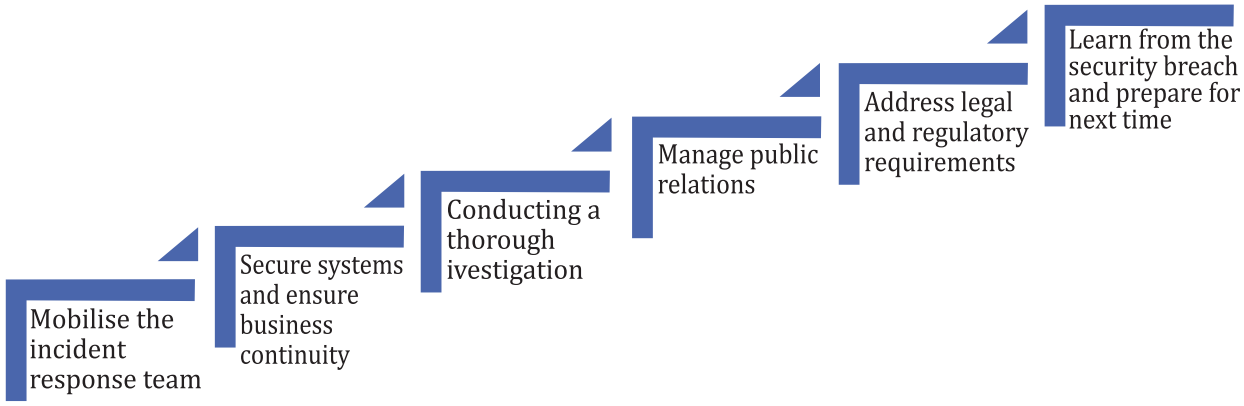
There are two types of companies – One who have experienced a cyber breach / cyber-attack and others who are going to experience a cyber-attack in future. It's not a question of IF, but only a matter of WHEN.

Cyber breach is no more only a technology issue but more a business issue as it affects every single team in the organization. Responding to a cyber-attack becomes the most important aspect of handling cyber security preparedness in any organization. When a breach is discovered, it is essential to act swiftly, or it may expose the business to greater liability. There are six critical steps the organization must take to deal with it.

It is important to bear in mind that these steps are not sequential – in practice, it will be necessary to think about most of them in parallel, particularly in the initial aftermath of the breach where the priorities will be to contain it in order to mitigate any risk of further damage or loss of data.

Handling immediate aftermath is critical for both your brand and your customers because one of the biggest concerns facing a business that's been compromised is maintaining customer confidence.

As we saw with Facebook's recent scandal over the misuse of user data, there is a huge amount of trust that the public places in the hands of data-capturing organizations. In the aftermath, Facebook's stock dropped £25 billion and a campaign to 'delete Facebook', instigated by high-profile users of the platform, went viral. Consequently, Facebook's reputation is far different now than what it was a year ago.



1. **Mobilise the incident response team:** Ideally every organisation should have an incident response team well in advance which should be immediately invoked in an event of an eventuality. This team should have representatives from cross functional teams including IT (Networking, Applications, Infrastructure), HR, Legal, Security with an interface with senior management.

   In case the organisation does not have internal skilled employees and adequate technology to deal with cyber-attacks they should have qualified technical partners / vendor community who can support them in managing the crisis on their behalf. Empanelment of vendors should be done proactively as time is critical.

2. **Secure systems and ensure business continuity:** Credentials for the important online accounts and servers where you keep your data needs to be changed.

   The organisation has to isolate or suspend affected section of its network, servers, machines temporarily or possibly even the entire network.

   One needs to also find out how and when the breach was detected and if any other systems have been compromised

3. **Conducting a thorough investigation:** The organisation should have a process in place to carry out investigations – root cause analysis of the incident. The organisation should have adequate resources, skills and expertise to conduct a in-depth investigations.

   Where there is potential employee involvement in the breach, the investigation will also need to take into account any applicable labour laws, and the investigation team should therefore consult and involve HR representatives as appropriate.

   Finally, the investigating team will need to ensure that they document any and all steps taken as these may be required as part of any regulatory notification to be submitted.

4. **Manage public relations:** One should be extremely cautious while doing this as one wrong statement or over statement can affect the image of your company in seconds. Along with the PR one should also manage the social media and needs to educate their employees of what they should avoid posting as this is crucial time as the entire world may be watching them.

   Being timely in managing announcements to the public and being accurate, open and honest in the messages given are crucial.

   The Global Data Protection Regulation (GDPR), which came into force in May this year, has fundamentally changed how organizations must respond to a cyber attack. The onus is on organizations to report any cyber attack to the authorities within 72 hours or face hefty fines.

   GDPR essentially forces companies to go public with any cyber attack they suffer, which poses further challenges when it comes to protecting their reputation.

5. **Address legal and regulatory requirements:** The Government of India, has established and authorised the Indian Computer Emergency Response Team (Cert-In), to collect, analyse and disseminate information on cyber incidents, provide forecast and alerts of cyber security incidents, provide emergency measures for handling cyber security incidents and coordinate cyber incident response activities.

   The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (Cert-In Rules) impose mandatory notification requirements on service providers, intermediaries, data centres and corporate entities, upon the occurrence of certain 'cyber security incidents'

   Upon the occurrence of any of the aforementioned events, companies are required to notify the Cert-In within reasonable time, so as to leave scope for appropriate action by the authorities. However, it is important to follow 'breach notice obligations', which would depend upon the *"place of occurrence of such breaches"*, and whether or not Indian customers have been targeted. The format and procedure for reporting of cyber security incidents have been provided by Cert-In on its official website.

6. **Learn from the security breach and prepare for next time:** One of the important aspect of recovering from a breach is to learn from the mistakes of the past and incorporate the best practices to further avoid the breach in future. The learnings will have to be incorporated in the updated policies, procedures, SOP's and the employees need to be trained to follow the updated policies and procedures keeping in mind that hackers and criminals are watching them continuously

   We need to test our employees regularly and also have a periodic review of our systems and processes by a external security consultant / auditor who comes with a fresh perspective and tells us what we cannot see or smell as we are a part and parcel of the furniture every day.

Cybersecurity best practices / cyber security essentials

1. Implement a formal is governance approach
2. Implement network segmentation, implement firewall, install antivirus
3. Detect and monitor unauthorized user behaviour to prevent data loss by insider
4. Use secure access methods like VPN technology for remote access
5. Implement role-based access controls
6. Backup data
7. Implement employee cyber security awareness training programs
8. Conduct periodic vulnerability and penetration testing of it infrastructure, update software and systems
9. Document and implement information security policies and procedures
10. Create and maintain incident response program

Chapter 9

About this Survey

This report is written by Netrika Consulting India Private Limited (Netrika) based on survey conducted by Netrika and prevalent acts and guidelines.

About Netrika Consulting India Private Limited (Netrika)

Netrika is a professional risk and integrity Management, an ISO 9001:2008 and 27001:2013 certified company, established with a vision to help the clients to focus on their core competencies in a risk-free environment with our experience of more than 3 decades across all industries throughout the globe. It is a professional risk and integrity management company that operates in emerging and frontier markets to advise clients on operational or business risks. With experience of completing challenging projects in all parts of the world, with operating offices in India, Sri Lanka, Singapore & Dubai, specialised in Corporate Investigations, Safety & Security Audits/Assessments, Intelligence Gathering and Risk Consulting.

Netrika's Cyber Security Advisory Services Vertical specializes in designing and implementing a robust Data Protection and Data Security Framework. The team provides practical and implementable solutions for detection, prevention, monitoring, incident response and investigations for the emerging cyber threats. Netrika's In-depth technical expertise in cyber forensics coupled with rich domain understanding have helped several customers around the world save millions of dollars and stay competitive.

About Authors

Contributors at Netrika Consulting & Investigation

Conceptualisation, research, content writing & editing

- Mr. Sanjay Kaushik – Managing Director
- Ms. Jyoti Khetarpal – Head - Forensics & Investigations
- Mr. Vaibhav Pulekar – Business Head - Cyber Security
- Mr. Vitul Gupta – Assistant Manager - Forensics & Investigations
- Mr. Mohnish Gahlot - Information Security Consultant

"Cyber Security refers to the use of protocols, best practices and technological solutions designed to ensure information and infrastructure is protected from cyber threats (emanating internally or externally).

The threat landscape is continuously evolving. We have moved from a world where a computer virus was the only major cyber threat to an era where advanced forms of attacks manifest every day. Ransomwares, zero-day attacks, phishing scams, data breach incidents have become extremely recurrent. Businesses and state actors have, therefore, started to take notice and put more focused governance and regulatory mechanisms in place.

Though cyber security has started garnering a greater pie of overall budgets year-on-year, India has miles to go in terms of cyber security infrastructure preparedness. With attacks getting smarter and more sophisticated, the need of the hour is to set up a more business focused security architecture and to institutionalize a cyber aware culture."

– Saurab Kaushik
Head Cyber Security, Lupin Limited

Notes

Notes

Our Presence

DelhiNCR:
Netrika Consulting India Pvt. Ltd.
Plot # 2, Industrial Estate,
Udyog Vihar, Phase - IV
Gurugram, Delhi NCR

+91 124 2883000
info@netrika.com

Mumbai
Netrika Consulting India Pvt. Ltd.
Accord Classic 510, Arey Road,
Goregaon East, Mumbai - 400063

+91 22 65104777
pravin.parab@netrika.com

Bangalore:
Netrika Consulting India Pvt. Ltd.
Unit No 205 A, Carlton Towers,
01 Old Airport Road, Bangalore

+91 80 43728750
sanganagouda.dhawalgi@netrika.com

Other India Offices: Chennai, Hyderabad & Kolkata

Singapore:
Netrika Consulting &
Investigation
JTC Summit,
8 Jurong Town Hall Road,
24-05, Singapore - 609434

+65 87308006
singapore@netrika.com

Srilanka
Netrika Consulting &
Investigation
32 Uswatte Road,
Etul Kotte, Kotte
Sri Lanka

+94 77 3410254
srilanka@netrika.com

UAE office
Netrika Consulting FZC,
SAIF ZONE,
Q1- 06 - 141/C
PO Box 124932,
Sharjah Airport Free Zone

+971 553794260, 525346993
dubai@netrika.com

NETRIKA CONSULTING & INVESTIGATIONS

Plot # 2, Industrial Estate,
Udyog Vihar, Phase - IV
Gurugram, Delhi NCR

www.netrika.com +91 124 2883000 info@netrika.com