USA's PROTECTION MEASURES TO STOP CYBER-CRIME

More than ever in the history of cyber-crime, USA has encountered numerous breaches over the period of pandemic. Every single work is done on internet and the developments in technology is both promising and alarming. The rate at which the cyber-crime has increased shows us clearly that our security needs to be tightened and certain laws are absolutely essential if businesses have to survive.

When a breach occurs in an organisation, the business suffers financially, emotionally and its reputation gets damaged in the process which often leads to major loss of customer support,withdrawal of investors and stakeholders. It becomes physically impossible for an organisation to stand again amidst the odds. Few companies in the past have lost their existence in the market and thus never have recovered, like Yahoo.

To provide protection to organisations from such malicious cyber-attacks, government has taken some strict measures against the cyber-crime. US Cyber-security laws and regulations cover some common matters and focus its attention on criminal activity, corporate governance, insurance matters and law enforcement jurisdiction. But it is considerable to think how hard it is to detect a crime and proof when everything is done abstractedly over the internet. Let's have a discussion about this.

WHY IT IS DIFFICULT TO SET A TRIAL AGAINST CYBER-CRIMINALS IN THE LAST CENTURY?

It is common and reasonable to consider the difficulties that arise while filing a trial against cyber-crime and the idea that to catch these criminals over the internet is a more challenging task than any other. Here are a few difficulties that arise during the process of denunciation.

STAGNATION

In the previous century, copyright laws protected the organisations for longer time, but as the century is progressing and the coming of the digital age shows us the need of better laws and better enforcement them.

Since the beginning of the digital era, the cyber-crime was quite meagre at that time, and as the time is progressing, the complexity is broadening with a serious threat that lurking for all businesses. The previous laws could not protect us anymore and that's why the stagnation needs to end with the arrival of new law enforcement.

AREA OF JURISDICTION

Many a times, it has been seen and observed that the person who has committed the cyber-crime is outside the legal Jurisdiction of court. Therefore, United States now has focused on international stage of area and has established allies all over the world to catch them.

UNREPORTED CYBER-INCIDENTS

Whether it is large or small business, the fear of losing the customers and industry allies and investors due to a cyber-attack is always justified. The reputational damage that is caused leaves many organisations cripple and thus, many the firms choose not to report the incident to the government institutions.

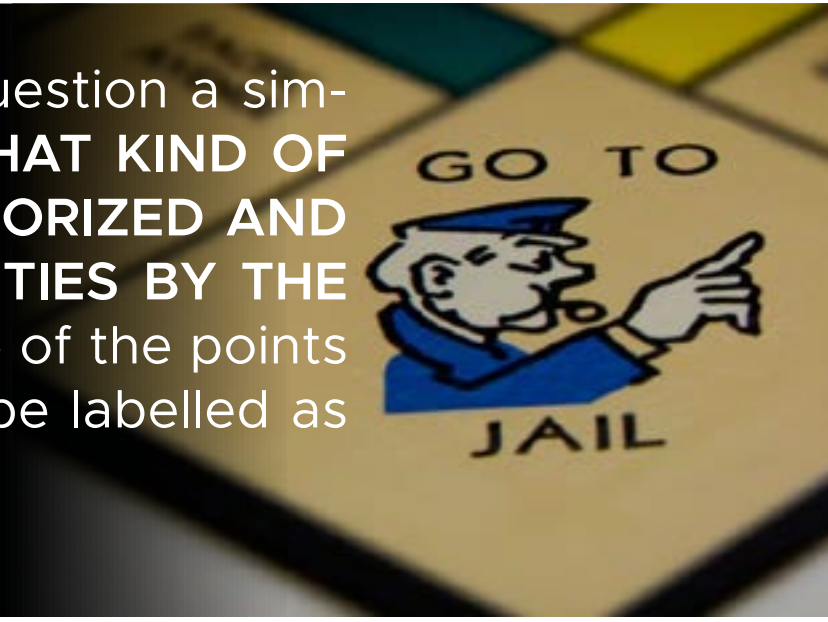
EVIDENCE COLLECTION IS QUITE CHALLENGING

It has often been seen that the evidence that is required to file against a cyber-incident often lacks because mostly employees delete that file or mail that caused the breach to occur at the first place. The human element turns always to be the most dangerous one, as once evidence is removed; no action can be taken against the criminals. Therefore it is advisable to conduct employee training and drilling in the organisation to ensure that everyone will perform their roles and responsibilities correctly when an actual breach occurs.

ADVANCING METHODS OF CYBER-CRIMINALS

It definitely requires a detailed planning and efficiency to conduct a cyber-attack and cyber-criminals work tirelessly in covering their tracks during the incident of breach. Tools such as TOR and VPNs allow hackers to change their domain area and to operate with a certain degree of anonymity. Cyber-criminals research every aspect and work continuously to be more challenging to identify, tack and apprehend. Thus, it is also our duty to advance our organisations up to that security level and to predict their moves in time.

A general curiosity arises when we question a simple but yet complex to formulate; **WHAT KIND OF CYBER-ACTIVITIES THAT ARE CATEGORIZED AND INCLUDED AS THE CRIMINAL ACTIVITIES BY THE US GOVERNMENT?** Let's look at some of the points which are deliberately considered to be labelled as cyber-criminal activity.



COMPUTER CYBER-HACKING

Any activity to break passwords or breaking strict security programs for any reason has been considered to be a major criminal activity.

ECONOMIC ESPIONAGE

Under this criminal activity, cyber-criminal spies keeps an on customer's credit card details, bank account details or any information they hacked to gain money illegally is considered to be punishable by law of cyber-security rules and regulations.

CORPORATE ESPIONAGE

Due to high competition and industry profits, at times some organisations have corporate spies to diminish the strength of the other competitors by any means, for example by stealing data, gaining the financial details or any progressing plans that the company under attack has.

IDENTITY THEFT

Any sort of activity in which an intellectual property is being stolen, or data or confidential information is considered to be a criminal activity under law.

MALWARE ACTIVITIES

The most common way or the tool that cyber-criminals use is by installing malware in their computer system, which in turn break through the computer system and gives unauthorised access to cyber-criminals. During this breach, they take all the information that is relevant or delete it so that the owner can't have access to that particular information that is being deleted by the criminals. Any such activity is also brutally punishable in the hands of the government.

STEALING CONFIDENTIAL DATA

Some data such as company's strategic growth plans, budget, employee's information, financial information,customer information is kept private and are only accessible by very few notable people in the organisation. Such information can be used as vulnerability by the cyber-criminals to breach and to use that confidential information for either their advantage or to exploit the company's growth and reputation. This kind of act is unbearable and severe actions must be taken to stop this, under some US laws, it is punishable by prison sentence.

UNAUTHORISED PUBLICATION

In the digital world, it is hard to keep a track of all the information and their copyright words, but laws have granted access to such information if it is used fairly by people, like in education. Likewise, it is a perplexing paradox to consider which type of information is punishable under governmental cyber-security laws. Here is an example, in case the information is used unfairly or confidential information becomes the victim of Ransomware attack, then at times, cyber-criminals leak the information to victimise certain companies to diminish their power of strength in the competitive market.

SPREADING OF FAKE NEWS

This is the most common issue which has been seeing and heard many times, through hacking the software systems, cyber-criminals spread some fake news about the company to damage its reputation. As we know, reputational damage is the mosst horrifying phenomenon for business as well as an individual; a company loses its customers, investor's as well as employees when a company suffers a reputational damage and financial obstacles to run the business. Any fake news of any sort can cause commotion in the office which in turn diverts them from focussing on their future plans; instead they have to deal with queries that aren't even true. It so obvious that these activities are punishable under the US government's laws and regulation.

SEXUAL EXPLOITATION

Sexual exploitation is no stranger to human socety, it has lived in the past, and keeps on showing itself that this kind of problem is one of the most common in all types of industry, place or even in houses. Under-cyber security laws, it has been stated that if anyone or cyber-criminals tried to break through an employee's information to sexually exploit them, is a straightaway prison sentence to those criminals.

CREATING IRRELEVANT TRAFFIC ON SITES

At times, cyber-criminals bring irrelevant traffic on the company's website, so that the main user will not get access to them in need. In this way, company suffers in providing services to their end-users. Customers never wait and why should they wait for one site to open when they have other sites that offer the same services. These type of cyber-criminals activity bocks the pathway for customers to reach to the company's website. This sort of activity is often being used for Ransomware purposes.

We just discussed numerous cyber-criminal activities which are punishable by law. At the very beginning of the digital phase, no-one have ever imagined that we humans will need protection laws for abstract entities. But now these abstract entities are the very foundation of how things work. The rise of the digital era made copyright intellectual rights a thing of the past and new regulations, laws are constantly on demand to provide protection against the evils of this technological epoch. Let us have a detailed discussion on some of the laws that US government is using to protect intellectual, financial and company rights for this digital era against cyber-criminals who continues to exploit its vulnerabilities.

LIST OF GOVERNMENT PROTECTION LAWS AND REGULATIONS: USA

SARBANES-OXLEY (SOX)

This law requires the organisations to prove that their credentials are true to its word. This law passed on 2002, since then, it is an important part of the cyber-security protection laws. This law has been named after bill sponsors U.S. Senator Paul Sarbanes and U.S. representative Michael G. Oxley, which resulted in SOX acronym. This bill requires the top management to certify the accuracy of the financial information. In addition to this, penalties will be taken on any fraudulent financial report or activity. SOX Increases the responsibility of boards of directors who are supposed to submit accurate corporate financial statements. SOX apply only to public companies which are being listed in a public stock exchange. A penalty could be very harsh if the financial information doesn't turn out to be right. A penalty of 1 million dollars and 10 or 20 years of imprisonment is being enforced onto the companies who wilfully submit wrong information while filing.

SEC REGULATION S-P

PRIVACY OF CONSUMER FINANCIAL INFORMATION AND SAFEGUARDING PERSONAL INFORMATION; SEC regulation requires for the organisation to take appropriate cyber-security measures. This law applies to U.S. brokers, dealers, investment companies, investment advisers which are registered and under the SEC regulation. The subject of the concurrent jurisdiction New York Department of Financial Services (NYDFS), these organisations are under the official obligation to report them of their financial statements and to adopt the written policies laid out by the NYDFS to safeguard data, records and protect against unauthorised access. FINRA (Financial Industry Regulatory Authority) is another body of institution that acts as a self-regulatory organisation for the financial Industries; FINRA is a private corporation that has the equal right of enforcing penalties to its subjects. SEC as well as FINRA has a contractual power to fine its members who violate this regulation can be made to pay $10, 98,190 or more.

GLBA GRAMM-LEACH-BLILEY ACT

GRAMM-LEACH-BLILEY ACT; this act is under both information security and privacy law. This law applies to all financial institutions such as banks, insurance companies, security firms, non-baking mortgage lenders, auto dealers and tax payers.

The GLBA security law requires all organisations to follow and adopt the comprehensive written program on information security and thus develop, implement and maintain administrative, technical and physical safeguards which are appropriate for the size and complexity of your organisation. This law safeguards the nature and scope of your firm's activities and customer's sensitive information. For violation of this law can cause a penalty of 1 million dollars and respectively the subject of the violation could also be removed or end their FDIC insurance which means the end of business from a financial firm.

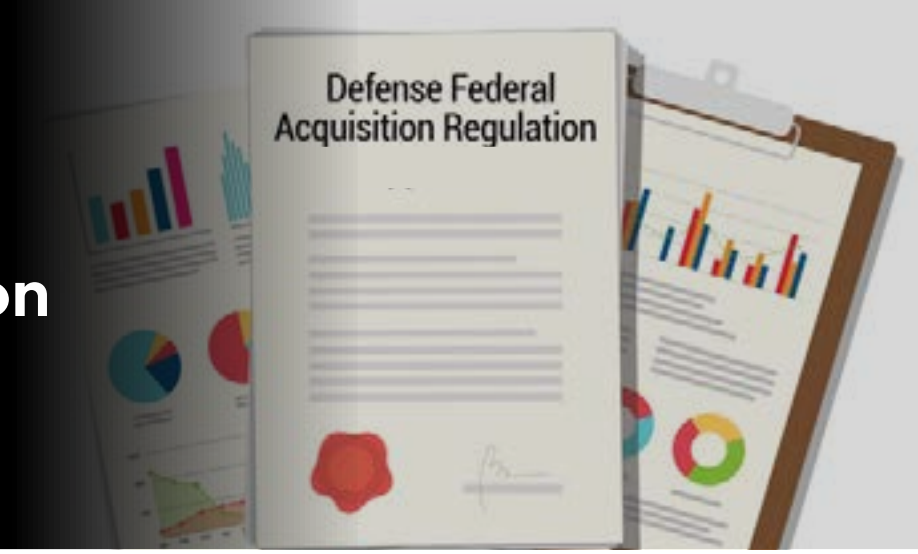
FTC
FEDERAL TRADE COMMISSION

This law requires proper follow up of information security regulation which states that organisations need to have appropriate cyber-security measures and a privacy law. This law is applicable to all types of organisations except of banks. FTC imposes some serious amounts of penalties onto its subjects for breaking this law and in the case of Facebook; FTC charged 5 million dollars concerning the recent case of violation. This law passed in 1914 to forbid unfair and illegal acts in the cyber-security privacy law in US.

HIPAA
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

This law has security, privacy and breach related rules which need to be followed. This law applies to health care industries, health care provider, health plans, health care clearing houses and to the businesses concerning with health care services. This Act covers diverse range of organisations from Heath care insurance companies to pharmaceutical companies. HIPAA has very specific rules for compliance. The violation penalty could change and it entirely depends on the seriousness of the crime committed. The largest fine being changed was $16 million and it has been dramatically increased in 2018 and reached to $28 million.

DFAR
Defence Federal Acquisition Regulation



DFAR applies to the US department of defence contractors in terms of cyber-security regulation. It requires the contactors and subcontractors of department of defence to store, transmit covered defence information to safeguard it from unclassified systems of operations. The penalty for violation of this act will result in the debarment.

COPPA CHILDREN'S ONLINE PRIVACY PROTECTION ACT

COPPA comes under privacy and cyber-security law. This law directs all its attention to the websites and online services used by the user under the age of 13. If the website owner knows that their site is being used by a minor, then it becomes an ethical responsibility of cyber-security laws to protect a minor user. COPPA ensures that these websites do not use these children's personal information for criminal purposes or to deceit or to exploit. This act is passed by the FTC with the largest fine to this day $5.7 million.

FDA REGULATIONS FOR THE USE OF ELECTRONIC RECORDS IN CLINICAL

INVESTIGATIONS

The Food and drug administration (FDA) regulations safeguard the use of electronic records in clinical investigations. FDA is a cyber-security law which applies to those organisations who are involved in clinical investigations of medical products, clinical investigators, including sponsors, institutional review board (IRB) and contact research organisations (CRO). This regulation concerns only the IT systems that these organisations use which includes any electronic system that these organisation used to create, record, modify, maintain, archive, retrieve, or to transmit records which are being used in clinical research.

CFTC
COMMODITY FUTURES TRADING COMMISSION
DERIVATIVES

This law CFTC protects the derivative markets, which includes Futures, swaps and different kinds of options. CFTC prohibits fraud trading activities in the trading of these contractual assets. The purpose of this law is to maintain integrity, resilience of the U.S. derivatives. It applies to derivatives clearing organisations. There are 27 such commodities worldwide which are being used as a medium for clearing transactions in communities for future delivery. For violation of this act can result in a heavy penalty that have to be paid up to $1,098,190 or more. The enforcement of this law is run by SEC and by FINRA.

ECPA AND SCA ELECTRONIC COMMUNICATIONS PRIVACY ACT AND STORED COMMUNICATIONS ACT

Electronic communications privacy act along with Stored Communications act, together they are called Wiretap act which comes under privacy laws and regulations. This act is designed to limit the use of unauthorised user domain. This act prohibits the intentional use, disclosure, access to any wire or electronic communication without authorisation. Violation of this act will lead to prison sentence.

EU-US PRIVACY SHIELD

European Union (EU) and United states formed a framework to regulate transactional exchanges for commercial purposes between them. The framework called the international safe harbour Privacy principles became invalid by European court of justice and replaced it with Privacy shield. The new privacy shield made significant improvements compared to the previous one, but still three main issues remained in the privacy shield. The European Data Protection Supervisor opined that the new shield is not strong enough to withstand future legal scrutiny before EU. Since US and EU exchange a lot of their information to this day, they come up with a program called safe harbour. Still this new program got over-turned by the ECJ (European Court of Justice), so EU commissioners and US government had to quickly come up with better alternative to meet the requirements of EU's General Data Protection Regulation (GDPR). The violation of this law or not adhering to this rule will lead to a fine of 20 million euros.

FPA
PRIVACY ACT OF 1974

Federal privacy act of 1974 applies only to those agencies which are the subjects of U.S. federal government. This act determines a fair practice of information that governs the collection, maintenance, use and dissemination of personally identifiable information regarding the individuals whose records are maintained by federal agencies. This law prohibits the use or disclosure of any recorded information about individuals whose records are the subject of federal agencies. For violation of this act will take the covered person to sue and will be obliged to pay the amount of the damage made, court fees and legal cost that are a part of the U.S federal district court.

CONSUMER PRIVACY PROTECTION ACT OF 2017

This act is directed towards protecting the privacy and security of sensitive personal data and to mitigate theft. It supplies important security notices regarding security breaches which involves sensitive personal information and it helps in enhancing law enforcement to maintain the protection of information security against cyber-breaches, fraudulent access, disclosure and, issue of personal information.The violation fine will not be more than $5 million unless the seriousness of the case is intentional.

Connect With Us -

(732) 347-6245

Email

service@iSmileTechnologies.com

Address: USA

241 Jonathan Way
Bolingbrook,IL 60490

India

2-3-285, Secunderabad
Hyderabad, 500003

Canada

3191 Stocksbridge Ave
Oakville, ON l6M 0A7

iSmile Technologies