DECEMBER 2018

THREATSPLOIT ADVERSARY REPORT

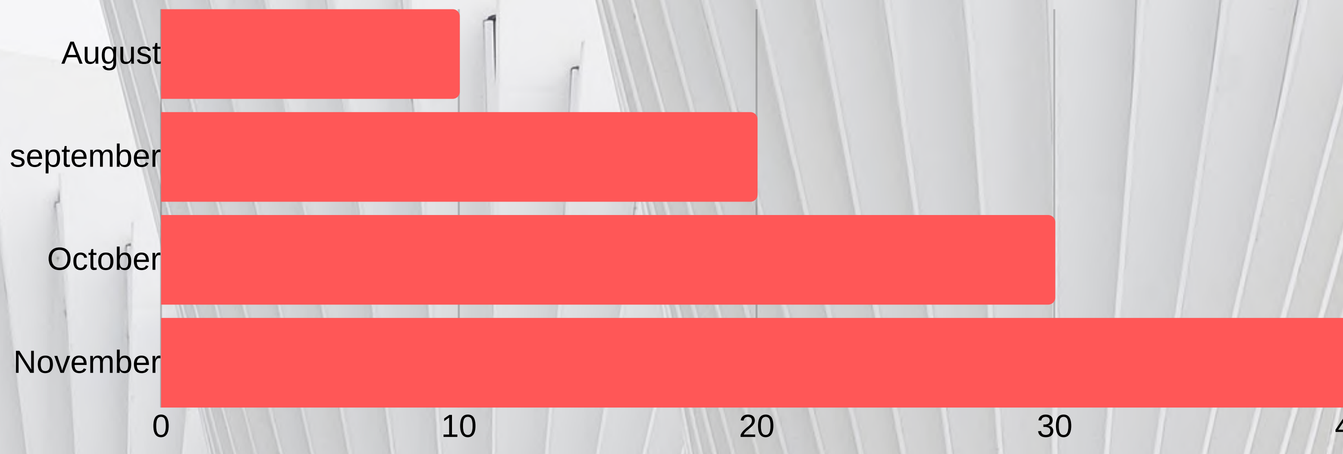
CONTACT US:
NM ROAD, CHENNAI
INDIA - 94

You can contact us at:
contact@briskinfosec.com
www.briskinfosec.com

BRISK INFOSEC
CYBER TRUST & ASSURANCE

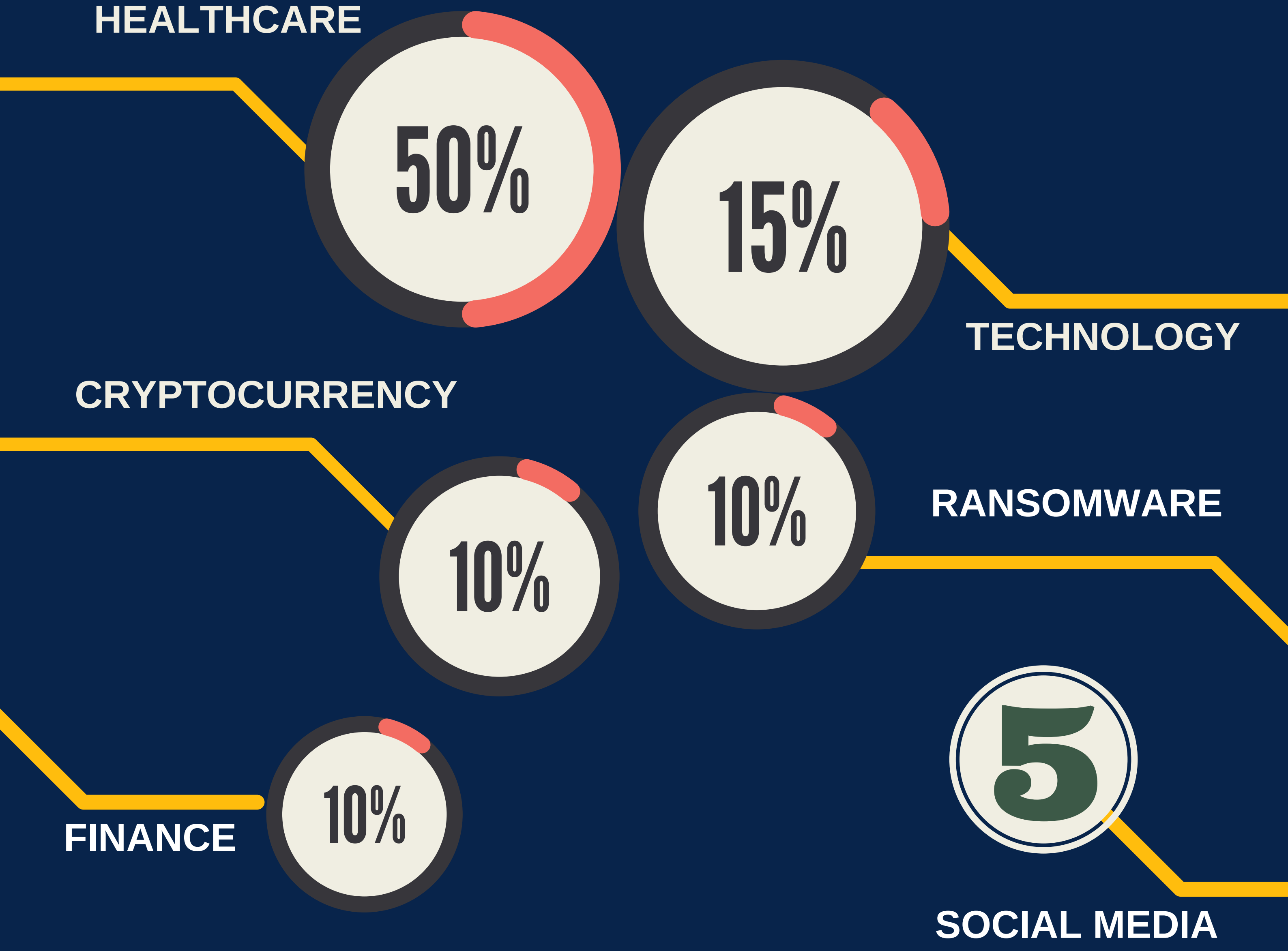
EXECUTIVE SUMMARY

On this auspicious occasion of upcoming christmas, we bring forth towards you the Threatsploit report which encompasses the ubiquitous cyber attacks that are reigning throughout the globe. Many organizations hear the news of various companies sparkling in the news as a victim of cyber attack. Despite the acknowledgement, due to complacent temerity, many companies neglect to upgrade their security parameters thinking it is just an one time implementation. Later when they themselves get their place scored as one among countless in the "victimised shore", radical stimuli of hiring a dexterous security vendor arises.The below graphical illustration demonstrates the fate of the late cyber issues which appears like never stopping and ever growing demons.



This threatsploit report is a result of Briskinfosec's untiring perseverance exclusively for cautioning all our noble clients and so, kindly have a perusal.

DATA STATISTICS OF NOVEMBER



HEALTHCARE 50%

TECHNOLOGY 15%

CRYPTOCURRENCY 10%

RANSOMWARE 10%

FINANCE 10%

SOCIAL MEDIA 5

Healthcare- needs care against cyber cracks.

Healthcare sectors have experienced the highest number of cyber breaches among others and these attacks are still on the rise. Are these going to be alleviated or ever proliferated. To prevent these, implementation of HIPAA (Health Insurance Portability and Accountability act) should be a must. Haven't you implemented it with a strong security assessment?

If not, call us now. We will prove us as the best in fullfiling your quest!

CONTENTS TABLE

HEALTHCARE

FINANCE

SOCIAL MEDIA

CRYPTOCURRENCY

TECHNOLOGY

- Amazon breach may have hit Indian users
- Amazon’s Technical Error Disclosed Customer Details
- Two New Bluetooth Chip Flaws Expose Millions of Devices to Remote Attacks
- New iPhone Passcode Bypass Found Hours After Apple Releases iOS 12.1
- Hackers find a way to access deleted photos on iPhones
- Chinese drones could be hacked to access videos and credit card details
- Here's How Hackers Could Have Spied On Your DJI Drone Account
- Bank Scam Using Google Maps loophole

RANSOMWARE AND CYBER CRIMES

- Targeted ransomware attacks surge in 2018: Report
- TalkTalk hackers jailed for cyberattack that cost company £77m
- India Saw 4.3 Lakh Cyber Attacks From Nations Including US, China: Report
- Report: Pakistani Air Force, Government Hacked
- New Stealthy Russian Hacking Tool Targets Government Agencies

FLAWS AND ZERO-DAY VULNERABILITY

- 7 New Meltdown and Spectre-type CPU Flaws Affect Intel, AMD, ARM CPUs
- Instagram Accidentally Exposed Some Users' Passwords In Plaintext
- Unpatched Virtual Box Zero-Day Vulnerability and Exploit Released Online

HEALTHCARE

4.4M Records Exposed in 117 Health Data Breaches in Q3 2018

Presented on nov 2018, Repercussions-4.4 M patients records breached on 117 healthcare data breached in third quater of 2018

On November 6th 2018, a total of 4.4 million patient records were compromised from 117 health data sectors, with the patient record numbers in 2018 increasing by whopping numbers from 4,597 to 2909,689 due to the apathy of insiders, reports Protenus. More than 50% of those hacks were due to hacking and 23% from insiders incidents, due to lethargy. Healthcare providers have also experienced breaches from 3rd parties accounting to 1.34 million breached records.Of the 117 health data breaches, 86 were disclosed by healthcare providers with 13 by health plan, 13 by disclosure from business associates and 5 being disclosed by business or other organizations. This incident exhausted 402 days to get disclosed. Virginia based VCU health systems breach took 5,605 days to be discovered with reason citing to be the easy access towards health information which encompassed names, DO's, medical record numbers and much more. When subjected towards states, Florida, California and Texas were leading as the distinct scapegoats of indistinct Data breaches.These breaches will be proliferating, unless the Healthcare organizations leverages contemporary technology services that enables in effectively auditing every patients data.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Multiple Attacks	Lack of Awareness	Reputation	Overall

HEALTHCARE

176.3 Patient Records Taken in Reported Breaches Since 2009

Presented on oct 2018, Repercussions-176.3 patient records breached on Helthcare centers since 2009

Hackers stole more than 50% of patients records among the 80% of unauthorized disclosure from 1,138 health care data breaches from 2009 to 2017, with half of breaches reported due to the firm's own mistake, according to a new JAMA Internal Medicine report. Researchers from Michigan State University and Johns Hopkins Carey Business school demystified that 2/3rd of security breaches from 133.8 million records were caused due to theft (or) from someone outside the organization. Researcher say that Healthcare entities must manage their plans in their security execution.Most corrective plans like encryption and restriction of mobile devices, enhancing physical security and digitizing PHI were strengthened. For those occurred in the cloud, remediation's like better monitoring, audit access and strengthening the firewalls were implemented. "Cyber security will have the greatest impact on the healthcare sector", reports JAMA with survey from 44 executives from 38 distinct health systems.Organizations flaunt in spending towards defending cyber attacks with survey. Survey says that employees apathy are the 62% reasons for biggest potential vulnerability, Nevertheless still employee awareness given the least precedence. Another survey indicates that 75% of hospital administrators were victimized by cyber attacks.The deal is not to seal with an impenetrable security but ensuring the implemented quality is extremely difficult to be broken.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Multiple Attack	Lack of Awareness	Reputation	Global

HEALTHCARE

HealthEquity Email Hack Breaches Data of 190K Patients

Presented on oct 2018, Repercussions-190k patients details breached on Health Equity, website-https://healthequity.com/

In November 20 2018, a second breach on Health Equity post their first breach in June was reported with compromises of 190,000 customers data, after an unauthorized user exploited two employee accounts.In an email to the HealthITSecurity.com, sophisticated methods such as bypassing the multi factor and device authentication were used for exploitation by hackers, reports officials. After detecting the attacks within hours, measures like passwords resetting, error correction and hiring forensics firm were levied as a proactive approach for protecting personal members information before the devil (hacks) strikes. The breached email accounts encompassed data's like names, health savings plan, social security numbers and much more. Databreaches.net obtained four different versions of notification letters from the Californian individuals. The 1st version reached 3700 Californians for notifying the breached social security number. The 2nd version reached 6000 Californians for notifying the breached employee names. In-spite of the Healthcare organizations providing a year of free credit monitoring, identity theft protection and $1 million insurance reimbursement policy. Health Equity President and CEO Jon Kessler apologized for this incident and we are working hard to make it right. As an Ulterior approach towards security, Health Equity has adopted best measures for preventing hacks, implementing security measures and is actively monitoring for suspicious detection.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Phising attack	Lack of Awareness	Reputation	USA

HEALTHCARE

Healthcare's Dependence on Fax Machines Poses Risk to Health Data

Presented on oct 2018, Repercussions-Fax machines poses risk on healthcare organisations

Being ignorant of physical data's disclosure could steer health care organizations to risk, In-spite of the various legacy devices often being used by them with more than 75% of healthcare communications being processed by outdated machines in healthcare sector, despite the prevalence of advanced technologies is truly, berserk and contemptible. Post the discovery of a "Cyber attack stimulation through fax number" kind of vulnerability, with contingencies for an hacker to easily launch it as revealed form the sources of Checkpoint researchers, it has further dreaded the security researchers in attaching personal data's to the recipient through faxes. All the 3 devices printers, scanners and fax machines are considered as office supplies and not a role of the management and tech team. As most fax machines are leased, it's taken after the lease period by the vendor and there may be data's impending in it, which would ensure high certainty for breaches to occur. These stuffs aren't even supervised by techies nor the management team and its arguably a huge risk for data beach risk.

Most infosec leaders are fully aware of the processes going on but they don't ensure the devices before being taken back by the vendor are free with all information erased, says Harstrick.

He concludes that, "Everyone focus on their living but none towards the end of their life".

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Memory Dumping	Negligence	Reputation	Global

HEALTHCARE

Health Data Breach Compromised PHI on 566K CNO Customers

Presented on oct 2018, Repercussions-half million CNO customers' data and a stolen employee laptop that exposed PHI on 10,000 Raley's pharmacy patients., website-https://www.cnoinc.com/

In November 20 2018, a second breach on Health Equity post their first breach in June was reported with compromises of 190,000 customers data, after an unauthorized user exploited two employee accounts. In an email to the HealthITSecurity.com, sophisticated methods such as bypassing the multi factor and device authentication were used for exploitation by hackers, reports officials. After detecting the attacks within hours, measures like passwords resetting, error correction and hiring forensics firm were levied, as a proactive approach for protecting personal members information. The breached email accounts encompassed data's like names, health savings plan, social security numbers and much more. Databreaches.net obtained four different versions of notification letters from the Californian individuals. The 1st version reached 3700 Californians for notifying the breached social security number. The 2nd version reached 6000 Californians for notifying the breached employee names. In-spite of the healthcare organizations providing a year of free credit monitoring, identity theft protection and $1 million insurance reimbursement policy. Health Equity President and CEO Jon Kessler apologized for this incident and we are working hard to make it right. As an Ulterior approach towards security, Health Equity has adopted best measures for preventing hacks by implementing proficient security measures and is actively monitoring for suspicious detection

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Unauthorized Access	Lack of awareness	Reputation	USA

HEALTHCARE

Phishing Attacks Breach Data of 42K Florida Patients for 3 Months

Presented on oct 2018, Repercussions-42Kk patients details breached in florida on Health First, website-https://healthfirst.org/

A Phishing attack compromised 42 K patients personal data's which was found out by a Floridian firm Health First on Nov 13th and was later reported to the Department of Health and human services. Data breaches.net revealed the hacked details of several employees between February and May 2018. Post the discovery of cyber attacks, Health First has implemented new security measures. Health first, perhaps the procrastination till October in reporting the breach to organization is the only one to report this news, despite many firms remaining unacknowledged of their breaches, hence obviously unreported. North Carolina-based Catawba Valley reported that 3 mail accounts had been accessed by hackers. Similarly, 37 K records of Gold Coast Health Plan were also breached. Another breach incident with compromises in 21 K patients records has made the Minnesota Department of human Services, in fire.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Phising Attack	Lack of awareness	Reputation	Florida

HEALTHCARE

Ransomware Attack on May Eye Care Breaches 30K Patient Records

Presented on oct 2018, Repercussions-30k patients details breached onMay Eye Care Center, website-https://mayeyecare.com/

Another popular Eye care firm named May Eye care on July29th has fallen as a victim of ransomware attack after its server, comprising of its patients names, birth, addresses, medical diagnosis, treatment details, clinical notes and insurance data's got breached.The patients included in the breached data were identified through 3rd party forensics and by IT security firms. These attacks are launched for extracting monetary payments. Officials have advised that precautious measures must be taken to secure the patients complete information. Inova health system in Virginia notified that 12,331 patients health data's records have been accessed by a hacker. Officials have confirmed that the same hacker has accessed both the billing system in January 2017 as well as in between July and October 2017 and also some paper records that contained patients names, addresses, DOB's, medical records and Social Security numbers in December 2016. Another prominent hospital in Texas, Altus Baytown was attacked by a ransomware on Sept 3rd, with health records being encrypted. The malware impacted not the electronic health record system but the files containing patients names, social security numbers and much more.Hackers demanded ransom for decrypting files. Officials said that these attacks were launched for extorting money and hence Altus firm have bolstered their cybersecurity defences by hiring outside security risk consultants.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Ransomware Attack	Targeted Attack	Reputation	USA

HEALTHCARE

VUMC Fights Healthcare Phishing with Multi-Factor Authentication

Presented on oct 2018, Repercussions- usernames and passwords on VUMC Healthcare university website-https://vumc.com/

Vanderbilt University Medical centre (VUMC), details its strategy for responding to mass phishing campaigns with added tech, user focused designed and education.Notorious viruses like Samsam and Ryuk have generated mayhems for health care sectors through various phishing attacks with one – hundredth of mails sent being malicious, reports FireEye researchers. VUMC hasn't escaped from this attack and hence urges for 2FA implementation for every tech org.Executive Director of Enterprise Cybersecurity Andrew Hutchinson to Health IT Security.com that despite the prevalence of 2FA for various platforms, VUMC had pushed this initiative ulterior, post the recent security threat. Hutchinson said that VUMC used phished sites which hackers used to gain access and so, ackers were able to view the contents while simultaneously being viewed by VUMC. Hence, for prevention 2FA (Two Factor Authentication) is necessary and for implementing it, there must be 100% involvement among employees as it increases the authentication levels of security and for sure will become a hard requirement for time, says Hutchinson. Success lies in providing comfortable situation to employees procuring plenty of opportunities for 2FA factor authentication, says Hutchinson.

EDUCATION AND USER-TRAINING:

He further added that humans made and will make mistakes and hence 100% success is impossible. There is no inevitable barrier against attacks but e are much better than 99% of organizations.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Multi-factor Authentication	Lack of Awareness	Reputation	USA

HEALTHCARE

Weekend Ransomware Attack Interrupts Care at 2 Ohio Hospitals

Presented on oct 2018, Repercussions-2 OHIO Hospital Ransomware onOHIO Hospitals, website-https://www.ohiohospitals.org/

Patients needing emergency care were driven away from East Ohio regional Hospital and Ohio Valley Medical Centre the weekend due to ransomware. The hired IT team took few computer systems for safeguarding the integrity of patients data's. "We have redundant security, so the attack was able to get through the first layer but not the second layer," Karin Janiszewski, OVMC and EORH director of marketing and public relations, told local news outlets. There has been no patient information breach. The hospitals are switching to paper charting to ensure patient data protection. At the moment, our emergency rooms are unable to take patients by E-squads, but we can take patients by walk-in. Our IT team is working around the clock right now and we expect to have the issue resolved by (Sunday)," Janiszewski said. Officials haven't provided an update on the attack. Throughout 2018, ransomware attacks have been breaching the security of various systems. In July, Cass regional medical centre consumed more than a week for its EHR, post a week after ransomware attack.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Ransomware Attack	Targeted Attack	Reputation	USA

HEALTHCARE

Phishing Attack Impacts Health Data of 128K Employees, Patients

Presented on oct 2018, Repercussions-Phishing attacks gives access to credentials of 128k employees on New York Oncology Hematology, website-https://newyorkoncology.com

Fourteen New York Oncology employees fell prey to the phishing attacks which gave access to credentials. The phishing emails appeared as legitimate email login page which conjured people and deceived them to log inside it. Post the Phishing attacks, the officials passwords were reset for the impacted emails. A forensic firm was hired, emails were reviewed by them and the NYOH were notified of the breaches, later launching incident response protocol. The concluded investigation on Oct 1st exposed the that the impacted emails contained names, email addresses, home addresses and much more. The officials must inform patients within 60 days under HIPAA to the DHS, but failed to do. As a remediation, all victims will be sent notification letters and a year of free credit monitoring. In fact, the Minnesota Department of Human services suffered due to spear-phishing campaigns with more than 1600 government emails victimized.Security researchers warn that attacks towards Healthcare sectors will only be rampant with time.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Phising attack	Lack of awareness	Reputation	USA

HEALTHCARE

NJ fines vendor behind Virtua Healthcare data breach $200K

Presented on oct 2018, Repercussions-Healthcare data breach-virtua agreed to pay fine of $200k, website

A fine of $200,000 was levied on Virtua as a result of its breached data's, by the New Jersey attorney general. By April, Virtua agreed to pay the fine and for improving its data security. In Jan 2016, Best Medical Transcription to Virtua experienced a sever misconfiguration that exposed the PHI of 1,654 Virtua patients. As a result, there were contingencies for files to be accessed and downloaded from the FTP site. In addition to this, even New Jersey's data's were breached. Their Attorney general Gurbir Grewal swore that, "Protection of New jersey's patients data's will persist". New Jersey's HIPAA's Security rule, Breach Notification rule and Privacy rule are cited below:

Failing to conduct an accurate and thorough risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI it held. Failing to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule.

Failing to implement policies and procedures to protect ePHI from improper alteration or destruction. Failing to notify Virtua of the breach of unsecured PHI Improperly using and/or disclosing ePHI in contravention of its obligations under its business associate agreement with Virtua.The state alleged that all the above rules constituted a separate violation of Consumer Fraud Act.Best Medical Transcription agreed to pay $30,508 within 30 days of settlement date. Later based on Mathur's agreement, the state has agreed to suspend the settlement balance.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Phising attack	Lack of awareness	Financial	USA

HEALTHCARE

Tullamore hospital hit by ransomware attack

Presented on oct 2018, Repercussions-15 employees fell victim to a phishing campaign, on Oncology Hematology, website-https://ohcare.com/

Dublin Midlands Hospital Group has confirmed an isolated ransomware attack at the Midlands Regional Hospital in Tullamore yesterday.

There was no impact on patient care following the attack, which affected the Laboratory Information System.There is also no evidence of other parts of the wider health service being affected by the attack, the group said.The hospital has been assured that there is no evidence it went any further and it is working with the HSE to restore the system.The group said business continuity plans are in operation until the full system is restored.The HSE have informed the Data Protection Commission as a precaution.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Ransomware Attack	Targeted Attack	Reputation	USA

HEALTHCARE

Data of 7,000 Tandigm Health Patients Exposed by Site Vulnerability

Presented on oct 2018, Repercussions-Patients data exposed by site vulnerability by unauthorized access, website-https://tandigmhealth.com/

A vulnerability in a website which was exposed for more than a period of 6 months from April 24th to December 31 2017 that exposed the personal data's of about 7k patients that include names, DOB, medical data and health insurance information, reports a Philadelphia based Tandigm on November 29th 2018.After the detection of vulnerability existence, a forensic team were hired for investigation to confirm whether data's were breached.Tandigm has enhanced its existing security features with better ones and staffs are also given awareness about issues. Further, the affected ones were offered 2 years of free credit monitoring and identity protection service.Another phishing attack on Georgia spine and orthopaedics of Atlanta corrupted the personal health information of 7k patients due to an unauthorized access in an employee email through phishing technique. Post acknowledgement, a forensic team were hired for investigation.The investigators figured out that the hack was contained to a single email account with patient names, Social security numbers and driver's license numbers being breached.2.6 million patient's records were breached due to a third-party billing vendor AccuDoc, with patient data's being compromised over a week, notifies Atrium health.This is the second time Health Equity has been beached this year.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Unathorrized access	security misconfiguration	Reputation	USA

HEALTHCARE

SSNs,Tax Data Exposed in Healthcare.gov Health Data Breach

Presented on oct 2018, Repercussions-Healthcate data exposed on ssns, website-www.healthcare.gov.

A Health data breach on Healthcare.gov portal abducted from there the Social Security numbers (SNNs), immigration status. The Centre of Medicare and Medicaid services (CMS) revealed the personal information risks of 75,000-94,000 individuals but concealed in revealing the information's compromised which contained names, DOB's, immigrant status, insurance plans and much more. A letter sent to the affected individuals from CMS, informed them that the account numbers, credit card numbers and the diagnosis of treatment data weren't accessible for the hackers and they promised in offering free identity theft protection services for the breach victims. The various persisting weaknesses were identified by GAO and in response to that, Republican lawmakers sent a letter indicating them to notify them about this complete issue. Todd park, former US chief technology officer was levied by the House Science, Space and Technology Committee in Oct 2014 about his role in developing the Healthcare.gov website. The committee Chairman Lamar Smith lashed out at Obama administration as, "What is the white House trying to Hide? The American citizens deserve to know their personal information". In July of that year, Healthcare.gov servers got breached, with review indicating that server didn't contain consumer's personal information. Also, further measures are implemented by them for security betterment.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Phising attack	Phising attack	Reputation	USA

FINANCIAL

HSBC Bank Data Breach Exposed Customer's Account Details and More

Presented on oct 2018, Repercussions-Exposed customer data and accounts details

A letter to the Californian attorney general's office was notified by the HSBC of the breached accounts which contained the name, all types of address, DOB, payee account information and much more. HSBC said that only 1% of its 38 million customers were breached. The breach may have happened through a technique called as "Credential Stuffing", a hacking technique with the assumption that same passwords are being used everywhere. More than 80% of U.S adults reuse the same password, from a 1000 people survey and this is the reason for the prevalence of "credential stuffing attack". Prevention is that users must regularly change their passwords. HSBC eradicated online access after being breached. The impacted customers were asked to contact them for seeking remediation's. After acknowledging the countless quantity of breaches, the European's General Data Protection Regulation requires companies to disclose personal data breaches to affected customers before 72 hours of becoming aware of them.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Credential stuffing	Improper access	Reputation	USA

FINANCIAL

Stolen data from 'almost all' Pakistan banks goes on sale on dark web

Presented on oct 2018, Repercussions-Pakistan banks goes on sale on dark web

Federal Investigation Agency (FIA) confirmed the shocking news that almost all the Pakistani banks were affected by a security breach, reported by FIA cybercrimes retired captain Mohammad Shoaib after acknowledging the shocking revelations of the credit and debit cards hosted Dark web forums. "More than 100 cases have been registered with the FIA and are under investigation," says captian Shoaib which contains 20,000 Pakistani data's hosted on the Dark web and even several infrastructure of Pakistani Banks compromised.Recent attacks indicate the need to improve the Banks security system. To implement better security, Al official's from the Banks were called for a meeting to limit the damages and to improve the security standards. Banks are the custodians of people's money invested an so Pilferage of those is an absurdity- Shoaib said. Last week a cyber attack on Bank Islami compromised 2.6 million from its accounts. Due to these attacks, Pakistani banks suspended usage of Debit cards as well blocked international transactions on their cards. Pakistan Computer Emergency Response Team (PakCERT) released a report with details such as Timeline and scale of leaks, the card skimming process used for Data extraction, the sales offered on the site JokerStash that contained over 11,000 records with more than 8,000 records pertaining to nine Pakistani banks.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Credential stuffing	Improper validation	Reputation	Pakistan

SOCIAL MEDIA

Private messages from 81,000 hacked Facebook accounts for sale

Presented on oct 2018, Repercussions-81k users facebook account for sale, website-www.facebook.com

Facebook reports that 120 million accounts were hacked with Facebook's data's, a part of it. Facebook later claimed that those allegations were false and it had taken steps to prevent hacks. Hackers offered to sell 10 cents per account with data's from UK, US, Brazil and elsewhere. Guy Rosen, Facebook executive said that malicious extensions have been removed from their site. Breach 1st came to light in September after a post from FB Saler appeared on English-language internet forum. Cyber security company Digital shadows said that over 81,000 profiles that contained private data's were posted online. With BBC Russian service contacting the 5 Russian victimized FB users and confirming it to be theirs. There were also hosted personal data's like talks between son in law and mother in law, chats between 2 lovers in St Petersburg whose IP address was later flagged by the Cybercrime Tracker service. Various applications are from various browsers like Chrome, Opera, Firefox as third party extensions. Cyber experts said that if rogue extensions were the cause, then the responsibility weighs over the developers. John Smith, an Anonymous source said that 2.7 million were of Digital Shadows said BBC that this claim was suspicious. Russian users out of 120 million and he revealed that information had nothing to do with Data leak. John Smith didn't advertise his services and when asked if the leaks were linked to Russian state or to the Internet Research Agency, with a grin he replied 'No'.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Malicious extensions	Targeted Attack	Repuation	USA

SOCIAL MEDIA

Instagram Accidentally Exposed Some Users' Passwords In Plaintext

Presented on oct 2018, Repercussions -Expose some users password in plaintext on instagram, website-www.instagram.com

According to The Information, Instagram has suffered a serious security leak of its own that could've exposed user's passwords. While Facebook recently had a much more serious problem linked to its "View As" tool that was being actively exploited by someone, the Instagram issue is linked to its tool that allows users to download a copy of their data. Facebook notified the affected Instagram users that when they utilized the feature, it sent their password in plain text in the URL. For some reason, these passwords were also stored on Facebook's servers, however the notification said that data has been deleted and the tool was updated so it won't happen now. In a statement to The Information, a spokesperson said the issue only impacted a "small number of people" although if those people were using a shared computer, or on a compromised network then it could've left their account info wide open. If you haven't been notified then your account apparently was unaffected, but it's still a troubling gap left in the hole of security, especially on something as important as passwords. While everyone should be using unique password managers for every site and service (if you need a password manager to keep up with them, then that's the way to go, meanwhile you can enable two-factor authentication on Instagram as described here), not everyone does and so an exposure of this kind is just another troubling episode to hit Facebook.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Data Exposer	Targeted attack	Reputation	USA

CRYPTOCURRENCY

Third-party JavaScript abused to steal money from Cryptocurrency exchange users

Presented on oct 2018, Repercussions - steal money from Cryptocurrency exchange users

Researchers at cyber security company ESET discovered that a Java script plugin was compromised through the injection of malicious scripts meant for targeting cryptocurrency exchanges. If detected, a second script replaced the victims bitcoin addresses with the ones used by attackers. Total losses of this attacks are unknown. Malicious injection of Java scripts through 3rd parties have been used to extract payment card data's through another technique, named as “Magecart”.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Crypto Mining Attack	Security Misconfiguration	Finacial	USA

CRYPTOCURRENCY

Four Fake Cryptocurrency Wallets Found on Google Play Store

Presented on oct 2018, Repercussions- Some apps found in play store were intentionally initiated for phishing attacks

4 bogus crypto-currency wallets were found through apps for NEO, Tether, Ethereum and Metamask on Google Play Store which tried to users personal data’s, reports an unanimous Blog. Those apps were intentionally initiated for phishing attacks. These wallets were distinguished into two as a “phishing wallet” (MetaMask) and as “Fake wallets” (other 3) by Stefanko.Stefanko in a video illustrated that “Fake Wallets” noted the example of fake NEO app “Neo wallet”, with over 1000 installs in it since October. The fake crypto wallets didn’t create a new wallet but displayed the attackers public address. These apps for development used Drag-n-Drop builder service, which means anyone can develop s trivial app for stealing data’s, reports Stefanko stating later that he even reported the fake apps to Google security team, with those wallets eventually being removed post acknowledgement. Coin-telegraph have reported that scammers compromised Google’s G suite and have reportedly spread an enticed message to stimulate users for participating in an illegitimate 10,000 Bitcoins takeaway.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Malicious App	User Account	Financial	USA

CRYPTOCURRENCY

Stat Counter Analytics Code Hijacked to Steal Bitcoins from Cryptocurrency Users

Presented on oct 2018, Repercussions-malicious java script detected on 7 lakh wbesites.

ESET malware researcher Matthieu Faou detected a malicious Java Script on 7 lakh websites, done with the connotation of Bitcoins pilferage. Post code analysis, researchers found the compromised StatCounter and replaced Java Script with malicious java Script. Perhaps the infliction of the contemporary malicious codes, script gets activated only when URL contains a specific Uniform Resource Identifier. The malicious script injected was intended to replace Bitcoin address destination to hackers address. Stat Counter successfully breached on Nov 3rd and was notified on Nov 5th labelling it as “supply chain”, as it appeared on service used by the target. StatCounter eliminated the malicious script on Nov 6th before the Gate.io stopped the usage of familiar analytic service on time. Gate.io also stimulated its customers to enhance security parameters through implementation of 2FA and 2 step login.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Cryptocurrency Hijacked	Phising attack	Financial	USA

TECHNOLOGY

Amazon breach may have hit Indian users

Presented on oct 2018, Repercussions-15 employees fell victim to a phishing campaign, on Oncology Hematology, website-https://ohcare.com/

US and UK were hit by data breaches which encompassed data’s like Names, email and much more. This incident is likely to panic Indian users where millions of users are desired towards Prime video and Prime music, with chances for Indian data’s to be breached. Amazon silenced their tensed customers by saying that their data’s are now secure and the issue has been fixed. More than 150 million users are there for amazon in India as of September 2018 with more users likely to join with the inception of localized products like Amazon Prime video and Shopping app in Hindi. User details falling into rogue hands while purchasing speakers, e-reading services when online can steer the user towards disastrous repercussions.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Malicious Attack	Security Misconfiguration	Reputation	USA

TECHNOLOGY

Amazon’s Technical Error Disclosed Customer Details

Presented on oct 2018, Repercussions-Disclosed customer details due to technical error, website-www.amazon.com

Customers information were disclosed during a busiest shopping period, says Amazon which also said that the issue was fixed and instantly emailed to all the victims. Amazon officials have said that no losses were incurred and Despite Amazon’s assurance, cyber security experts insisted customers to change their passwords for security betterment. Indeed the existence of GDPR (general Data Production regulation) for security, Amazon failed to disclose the incident. It is the company’s responsibility to identify the breached citizens and prevent them from enduring further harm, a spoke person said. Tech firms must provide transparent solutions to companies when problem arises, for earning the people’s trust.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Security Misconfigure	Improper configuration	Reputation	USA

TECHNOLOGY

Two New Bluetooth Chip Flaws Expose Millions of Devices to Remote Attacks

Presented on oct 2018, Repercussions-Bluetooth chip security flaws which allowed remote attacks.

Two critical vulnerabilities in Bluetooth low energy (BLE) chips were unveiled by the security researchers which allowed remote hackers to take full control of devices of any data’s through the execution of arbitrary codes. Discovered by researchers at Israel security firm, it was notified to be made by Texas instruments being used by Cisco, Meraki and by much more.CVE-2018-16986 the 1st vulnerability, sustains in TI chips CC2640 and CC2650 and many Cisco and Meraki’s Wi-Fi access points. The bug takes the extra edge of a loophole in the way Bluetooth chips supervise the processing data. According to the researchers, launching more traffic to a BLE chip causes memory corruption alias buffer overflow attack, which could allow an attacker to run malicious code on an affected device.“First, the attacker sends multiple benign BLE broadcast messages, called Advertising Packets.“Next, the attacker sends the overflow packet, which is a standard advertising packet with a subtle alteration, researchers explained. The 2nd vulnerability, notified as CVE-2018-7080, exists in CC2642R2, CC2640R2, CC2640, CC2650, CC2540, and CC2541 TI chips, and affects Aruba’s Wi-Fi access point Series 300, arising from a stem with Texas Instruments’ firmware update feature in BLE chips, termed as Over the Air firmware Download (OAD). Texas Instruments finalised the vulnerabilities and generated the security patches for affected hardware which can be made use through respective OEMsechanism of the firmware running on the BLE chip over a GATT transaction,” researchers explained.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Remote Attack	Security Flaw	Reputation	USA

TECHNOLOGY

New iPhone Passcode Bypass Found Hours After Apple Releases iOS 12.1

Presented on oct 2018, Repercussions-Bypassed iphone passcode on ios 12.1 on apple, website-www.apple.com.

An IPhone techy freak has bypassed the security features of it through malicious codes that allows viewers to espy the private information on the locked iPhone. Jose Rodriguez a Spanish security researcher confirmed that he discovered an iPhone bypass bug in the latest version in iOS 12.1, released by Apple today. Apple with iOS 12.1 released a new feature called Group face Time that enables users to easily chat with max 32 people. Unlike previous hacks, the new method functions without saving Siri or Voice Over screen reader and the steps to execute those are cited below:

Call the target iPhone from other iPhone Initiate the “Facetime” post call connection.

Now select ‘Add Person”+ icon and access the contact list with 3D enabling for more intimate perusal.

Since there’s no remedy for fixing the issue, until Apple issues a software update for bypassing the bug, users have to wait for it.Other than these, Rodriguez has discovered tow passcode bypass hacks in iPhone 12.0.1 and in iOS 12, with both taking advantage of Siri and Voice over screen reader, thus providing easy physical access to contacts and photos.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Bypassed	Phising attack	Reputation	USA

TECHNOLOGY

Hackers find a way to access deleted photos on iPhones

Presented on oct 2018, Repercussions-Exposing massive laws on iphone that gains access to recently deleted photos

Two white hackers have scored a massive $50,000 payout for exposing massive laws on iPhone X that gains access to recently deleted files.Richard Zhu and Amat Cam, through bug bounty found the loopholes in iOS’s just-in-time (JIT) compiler when connected to malicious Wi-Fi access point. Delete option in iOS doesn’t leave your phone exactly but sticks around your memory for 30 days.This made the hackers penetrate into the deleted images before a month and possibly even more. However perplexes are still unclear that is this flaw existing only for iPhone X or even for others.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Security Misconfuguration	Application Flaw	Reputation	USA

TECHNOLOGY

Chinese drones could be hacked to access videos and credit card details

Presented on oct 2018, Repercussions-Sexurity and privacy issues caused huge vulnerability

More than 70% of the global markets for personal, commercial and military use were supplied by the Chinese drone giant-Da-Jiang.Concerns are arousing about drone security and privacy issues.Checkpoint has cautioned the firms that a huge vulnerability has been inflicted in servers that could easily excavate the personal data’s of the personnel’s.Oded Vanunu, head of Check point’s threat prevention team said that the Hacker could access logs, photos, videos personal information, cards and much more by just inflicting a cookie that monitors the users activities.To add more fuel to the flame, another vulnerability with identification tokens was exploited to hack 50 million’s FB profiles in September.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Sniffing attack	Phising attack	Reputation	CHINA

TECHNOLOGY

Here's How Hackers Could Have Spied On Your DJI Drone Account

Presented on oct 2018, Repercussions-Sensitive data exposed view Dji drone

Vulnerabilities in DJI Drone web app were discovered and revealed by the Check Point today to DJI security team after 6 months of attack that held data’s on sensitive information, flight records, live video camera feed and much more.Advantage of 3 different vulnerabilities in DJI infrastructure including secure cookie bug in DJI identification process, XSS flaw and a SSL Pinning issue in its mobile app.Once captured, the login cookies takes control over DJI web account on its centralized drone operations management platform called DJI Fight hub.DJI classified the vulnerability as High, medium and low risks.DJI faced scrutiny in the US after the DHS (Department of Homeland security) released memo accusing the frim of sending sensitive information.
However the drone maker refused those allegations claiming it as a FAD.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Data Hijacking	Targeted Attack	Reputation	USA

TECHNOLOGY

Bank Scam Using Google Maps loophole

Presented on oct 2018, Repercussions-bank customers and thousands of data's scammed

A flaw was detected in Google maps through which bank customers and thousands of other data’s were scammed, thus revealing data’s like CVV and ATM pins. Due to this, Google proclaimed in terminating down its Google + division, reports The Hindu. They even stated that bank’s numbers were replaced by their rogue numbers through conning.Maharashtra cyber police articulated that people call these numbers in google maps thinking to be legitimate, with scarce people identifying the scammer that is detecting them stealthily and cajoling to reveal sensitive information’s.Bank of India has levied users to refer only contact details and not 3rd party sources. The have also modified their data’s on Google maps, reports The Hindu.Google safety Centre Outlines tips to enhance customers safety in online sources, says a Google spokesperson.Maharashtra cyber police revealed that whenever people searched for Bank online, the 1st search would be a google link with contingencies for higher number of victims count.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Scamming	Security Flaw	Reputation	USA

RANSOMWARE

Targeted ransomware attacks surge in 2018: Report

Presented on oct 2018, Repercussions-report of ransomware attacks in 2018

2018 saw the advancement of hand-delivered, targeted ransomware attacks that are earning cyber criminals millions of dollars, according to the Sophos 2019 Threat Report. The report, produced by SophosLabs researchers found that capitalist cyber criminals are turning to targeted ransomware attacks that are premeditated and reaping millions of dollars in ransom.The threat report explores changes in the threat landscape over the past 12 months, uncovering trends and how they are expected to impact cybersecurity in 2019.“The threat landscape is undoubtedly evolving; less skilled cyber criminals are being forced out of business, the fittest among them step up their game to survive and we’ll eventually be left with fewer, but smarter and stronger, adversaries. These new cyber criminals are effectively a cross-breed of the once esoteric, targeted attacker use manual hacking techniques, not for espionage or sabotage, but to maintain their dishonorable income streams. Cyber criminals are using readily available Windows systems administration tools as their route to advance through a system and complete their mission – whether it’s to steal sensitive information off the server or drop ransomware.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Ransomware	Targeted attack	Reputation	global

CYBER CRIMES

TalkTalk hackers jailed for cyberattack that cost company £77m

Presented on oct 2018, Repercussions- Two hackers jailed for cyber crime activities that cost 77 million

Two pals Matthew Hanley 23 and Conor Allsopp 21 were sentenced for 20 months due to their collaboration in the execution of a successful breach. The pair hijacked 156,959 customer accounts which comprised of personal, banking and sensitive data’s.The total cost of the TalkTalk breach which caused distress and mayhem to thousands, is estimated around $77 million.TalkTalk reported the cyberattacks to police and National crime Agency alerted the customers with Hanley described the name “Determined and dedicated hacker”.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
User Account Hijacked	Improper Validation	Financial	USA

CYBER ATTACKS

India Saw 4.3 Lakh Cyber Attacks From Nations Including US, China: Report

Presented on oct 2018, Repercussions-cyber attacks report on ondia 4.3 lakhs cyber attacks

A Finnish cybersecurity company said that India has been affected by over 4.3 lakh attacks initiated from 5 different companies. Moreover, even Russia, US, China, Netherlands and Germany have targeted India with 436,090 attacks, being more than 12 times originating from India.Russia accounted for most cyber attacks succeeded by US, China, Netherlands and even from Germany with Austria, Netherlands, UK, Japan and Ukraine targeting India with 36,563 attacks.Leszek Tasiemski, the vice president of cyber security products said that it’s becoming lucrative for hacking due to digitalisation. We are enhancing measures for protecting the evolving threat landscape, he added.Honeypots are explicitly used for grabbing attention of future victims and they gain insights on attack types, targets, sources and much more.F- Secure said that victims and even elite hackers find so hard in figuring out as an Honeypot as they appear to be serving organizations purposes.They even enable F-Secure products via customers for extracting latest malware samples, shell scripts and sometimes upbringing even new hacking techniques.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Multiple	Multiple	Reputation	India

CYBER CRIMES

Report: Pakistani Air Force, Government Hacked

Presented on oct 2018, Repercussions-Hacking tool targets goverment agencies

Foreign state-sponsored hackers infiltrated the security elements of PAKISTANI AIR FORCE, reports a private cybersecurity firm.Cylance first reported that a group named as “The White Company’, hacked various elements of Pakistan’s military and intelligence networks and says that more threats may strike the government.Spokesperson at the firm said that the attack could be launched from a Middle East with exact data’s about the attacks origin and the pilferage data’s unrevealed.Cylance and other private security firms have helped in detecting and publicizing various hack activities like the Stuxnet virus, developed by the US and Israel in 2006 for Sabotaging Iran’s nuclear program.Cylance said it shared about these threats with U.S government and PakCERT- a Non-Government organization like a computer emergency response teams.Officials at Cylance said that attack espionage was used for stealing sensitive Pakistani information, which was achieved through spear-phishing technique for gaining access to the secure data’s.Pakistan came under scrutiny as most of its banks were subjected to a wide-scale security breach.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Hijacked	Unknown	Reputation	USA

CYBER CRIMES

New Stealthy Russian Hacking Tool Targets Government Agencies

Presented on oct 2018, Repercussions-Hacking tool targets goverment agencies

Palo Alto Networks on November 21, 2018 discovered the “Cannon Trojan”, a new Russian hacking tool is targeting government systems in US and Europe through various stealthy attack modes, by using the AutoClose function that swiftly accomplishes its action through malicious codes. The virus acts a downloader.It is next delivered through an email as Word document. The Word document installs two malicious programs and then Cannon allows Hackers to gain the victims information.Palo Alto researchers believe Russian hacking group Fancy Bear or GRU whom were behind many successful attacks like Democratic National Committee and medicine data from both the International Association of Athletics federation and World Anti-Doping Agency were also behind this.The group has also been targeting US think tanks, government agencies and other business phishing campaigns. Due to lack of strong security resources, even Minnesota Department of Health and Human services suffered cyber impacts.

Healthcare sector suffered from several constraints, and even other sectors could suffer through the infusion of the contemporary evasive attacks.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Phishing Attack	Targeted Attack	Reputation	Russia

SECURITY FLAWS

7 New Meltdown and Spectre-type CPU Flaws Affect Intel, AMD, ARM CPUs

Presented on oct 2018, Repercussions-CPU flaws affect intel,amd,arm cpus

Meltdown and Spectre vulnerabilities affected a large family of modern processors through which sensitive data's can be gained. Since then more like Spectre NG, Spectre RSB, Spectre 1.1, Spectre 1.2, TL Bleed, Lazy FP, Net Spectre and Foreshadow were released.Speculative execution- a mandatory component of modern processors executes instructions based on assumptions that are considered with a hope to be true. If the assumptions are valid, the execution continues, otherwise discarded.The same team who found Meltdown and Spectre vulnerabilities have discovered 7 new transient attacks that impacts 3 main processors like Intel, AMD and ARM.Those 7 recently discovered attacks are listed below:
Meltdown-PK – A protection key bypass
Meltdown –BR _ Bounds Check Bypass
Spectre-PHT _ Pattern History Table
Spectre PHT CA OP – Cross address space out of Place
Spectre PHT SA IP _Same Address space in place.
Spectre-BTB-SA-IP _ Same Address-space In Place
Spectre-BTB-SA-OP - (Same Address-space Out of Place.

Researchers disclosed their findings to Intel, ARM and AMD with Intel and ARM knowing the report. Further vendors were working to finding best fixes with best of time.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Security Misconfiguration	lack of Awareness	Phising attack	spain

ZERO-DAY

Unpatched Virtual Box Zero-Day Vulnerability and Exploit Released Online

Presented on oct 2018, Repercussions-Zerpo day vulnerability expolit

An oracle zero day platform independent vulnerability, which affects versions till 5.2.20 and allows malicious files for bypassing and exploit OS were released by a resented researcher.The vulnerability arises due to memory corruption issues with the security researcher claiming that it either works or never works and works in Ubuntu 16.04 and 18.04 x86-64 configurations.The researcher took an oath and disclosed the data's due to his wrath on Oracle when he reported similar issue last time. As of Nov 8th 2018, patch wasn't available and hence metamorphosing virtual ethernet Card to PC net and changing network mode to NAT would help in restricting the exploit to a considerable extent until a best patch gets its inception.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
zeroday vulnerability	Targeted Attack	Reputation	USA

CONCLUSION

Various security breaches have been reported. The main reasons for these are

- Improper security mis configuration.
- Using piracy and non-indigenous software.
- Lack of awareness of the past, present and about future issues.
- Implementing cyber security laws without compromises.
- Failure in identifying Fake security configurations.
- Usage of weak passwords.
- Last but not the least, negligence in hiring a competent cybersecurity firm due to complacency.

Just like a little quantity of poison paralyses and kills many aqua-lives, every tiny cyberattack on small and big organizations makes their name shine in a waning moon for "Hacked" or "Victimised" reasons, thus annihilating their reputation. All these are due to the avoidance of proactive approach towards security, primarily due to complacency and because of the absurd feeling "Our security is Inevitable", which later becomes as ephemeral after being compromised inevitably.

"Prevent attacks by implementing best
Lament never after enduring worst"!

Reference link

- https://healthitsecurity.com/news/4.4m-records-exposed-in-117-health-data-breaches-in-q3-2018
- http://www.247healthnews.net/2018/11/20/176-3-patient-records-taken-in-reported-breaches-since-2009/
- https://securenetmd.com/feed-items/healthequity-email-hack-breaches-data-of-190k-patients/
- https://healthitsecurity.com/news/healthcares-dependence-on-fax-machines-poses-risk-to-health-data
- https://svpn.com/health-data-breach-compromised-phi-on-566k-cno-customers/
- https://www.healthcare-informatics.com/news-item/cybersecurity/health-first-data-breach-exposes-information-42k-patients
- https://www.hipaajournal.com/30000-patients-impacted-by-may-eye-care-center-ransomware-attack/
- https://www.healthdatamanagement.com/news/vanderbilt-to-leverage-multi-factor-authentication-to-thwart-hackers
- https://securitytoday.com/articles/2018/11/29/ohio-hospitals-disrupted-by-ransomware-attack.aspx?m=1
- http://www.247healthnews.net/2018/11/19/phishing-attack-impacts-health-data-of-128k-employees-patients/
- https://patch.com/new-jersey/gloucestertownship/200k-settlement-reached-virtua-database-breach-ag
- https://www.irishexaminer.com/breakingnews/ireland/tullamore-hospital-hit-by-ransomware-attack-885693.html
- https://www.hipaaguide.net/phi-of-7000-patients-exposed-due-to-tandigm-health-website-vulnerability/
- https://www.digitaltrends.com/web/healthcaregov-breach-data/https://hackercombat.com/hsbc-bank-data-breach-exposed-customers-account-details-and-more/
- https://securityaffairs.co/wordpress/77847/cyber-crime/pakistani-banks-data-breach.html
- https://www.bbc.com/news/technology-46065796
- https://www.engadget.com/2018/11/17/instagram-password-data-bug/
- https://www.systemtek.co.uk/2018/11/third-party-javascript-abused-to-steal-money-from-cryptocurrency-exchange-users/
- https://www.investing.com/news/cryptocurrency-news/four-fake-cryptocurrency-wallets-found-on-google-play-store-1689086

BRISK INFOSEC

CYBER TRUST & ASSURANCE

THREATSPLOIT ADVERSARY REPORT DEC 2018

WWW.BRISKINFOSEC.COM