TECHNOWHIZ

ACCREDITED WITH GRADE A++ NAAC IN 2nd CYCLE

jims
Sector - 5, Rohini, Delhi

ECHELON

THE HORIZON OF INNOVATION

SHAPING CYBER-READY TECHNOCRATS

CYBER SECURITY

BCA Annual IT Magazine 2026

Message *from* the Principal

A college magazine offers something beyond ink on paper, it is the embodiment of the curiosity, the ambition, and the restless energy that defines student life. It captures what a classroom often cannot– the unscripted moments, the vibrant and bold ideas, and the ever creative spirit that quietly shapes an institution's very identity.

It gives me immense pleasure to celebrate the release of Echelon (2026), brought to life by the dedicated faculty and the students of Bachelor of Computer Applications (BCA). With each edition that is brought to life, this magazine grows not only in its depth and character, but in its ability to reflect the ever evolving, and introspective soul of the department. This year's edition is no different, it stands a proud chronicle of talent, perseverance and collective vision. I extend my heartfelt congratulations to the entire Echelon team for their earnest efforts in bringing this vision to fruition.

Those who dare to dream, and more importantly, the ones that are willing to work towards that dream with sincerity and grit, are the ones who ultimately leave their mark on the world. The value of education lies not only in what it teaches you, but what it enables you to become.

As Steve Jobs once said, *'The people who are crazy enough to think they can change the world are actually the ones who do it.'*

Let your education be the force that makes you one of them.
My best wishes to the entire Echelon team for continued success and all future endeavours.

Dr. Praveen Arora
Principal
JIMS

Message *from* the Editors

Ms. Rupakshi Gaur
Assistant Professor
JIMS

Dr. Shivani Vats
Assistant Professor
JIMS

Every year, as the pages of our college magazine take shape, it is a reminder of something timeless, that learning is never confined to textbooks alone. It breathes through stories, through art, through the quiet confidence of a student who finds their voice on a blank page.

Echelon (2026) is a testament to exactly that, and it gives us great joy to see it come to life once again. This edition did not come together on its own, it was built on late conversations, reworked ideas, and a shared belief that what we were creating was worth the effort. To every student who contributed, your dedication, hard work, and unwavering commitment have been the driving force behind this endeavour.

Each of you brought something unique to the table, and it is that diversity of talent, and perspective that makes this edition truly special. The efforts, countless hours, the late nights, and quiet sacrifices that went into these pages do not go unnoticed, they are seen, and they are deeply appreciated.

Thank you for your passion, your resilience and for making this edition what it is.

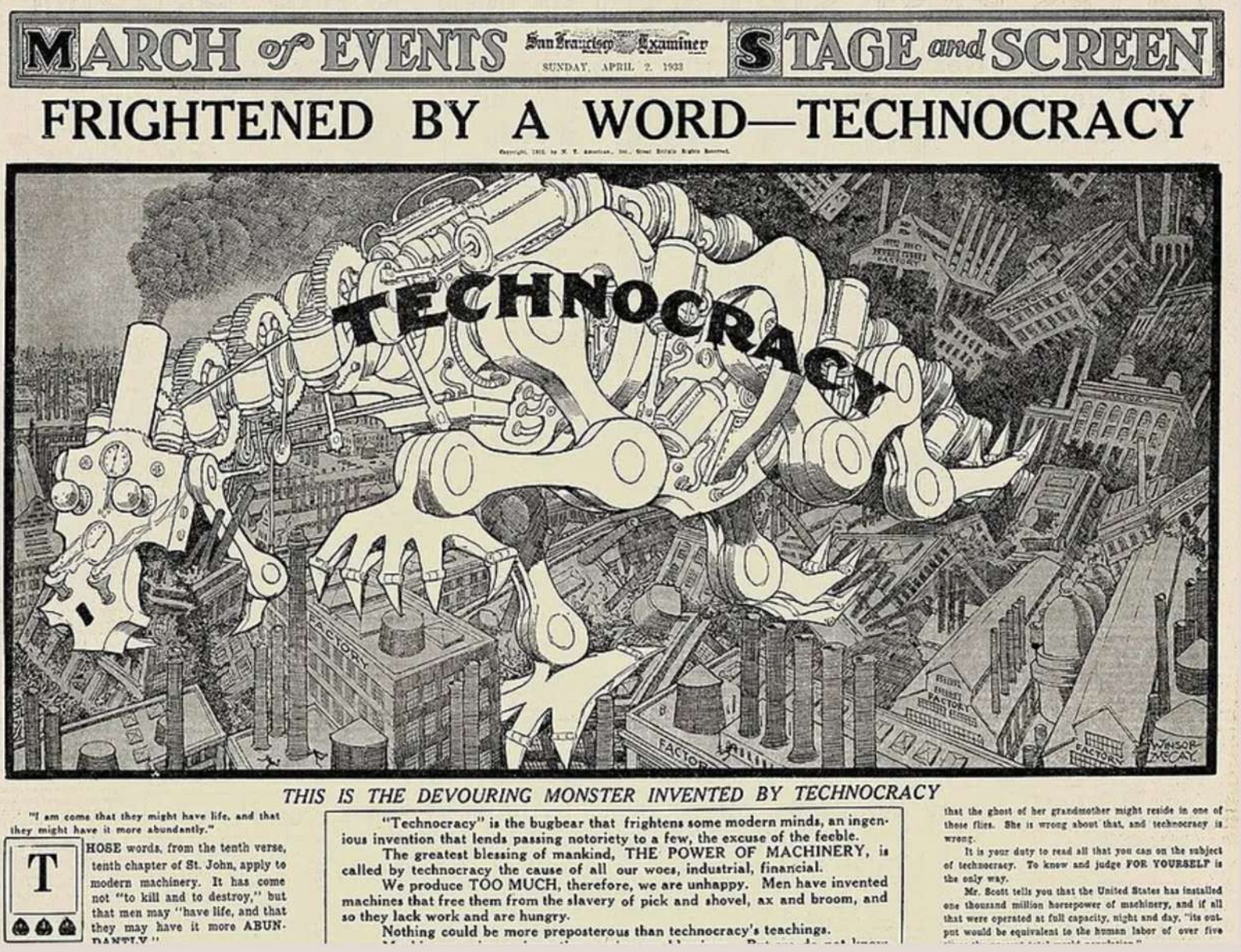
May this be one of many things you look back on with pride.

With sincere appreciation,
Ms. Rupakshi Gaur and Dr. Shivani Vats

TABLE OF CONTENTS

		PG NO
1	Technocracy in the Changing Technological Landscape	01
2	The Cyber Mindset Shift	03
3	Foundations of Cyber Thinking	05
4	Building a Cyber First Mindset	07
5	Secure-by-Design Mindset	09
6	Prevention Over Patch Culture	11
7	Human Error : The Weakest Link	13
8	AI Systems and Cyber Exposure	15
9	Everyday AI Threat Landscape	17
10	Digital Footprints and Identity	18
11	The Cost of Cyber Negligence	19
12	Mixpanel Vendor Hack	20
13	Escaping the Cyber Myths	22

		PG NO
14	Cyber Psychology and Human Behaviour	24
15	Bybit Crypto Heist	25
16	The Wonders of DNS Poisoning	27
17	What Breaches Teach Technocrats	29
18	Bridging the Cyber Skill Gap	30
19	Military AI and Ethical Boundaries	32
20	The Google Vishing Breach	34
21	Ethics in AI and Cybersecurity	35
22	The Indian Context	37
23	Security in Emerging Technologies	38
24	What a Quantum Future Means for Cyber Security	39
25	Cyber Security and Innovation	41
26	Feature : AI Summit	43



MARCH of EVENTS — San Francisco Examiner — SUNDAY, APRIL 2, 1933 — STAGE and SCREEN

FRIGHTENED BY A WORD—TECHNOCRACY

TECHNOCRACY

FACTORY

FACTORY

FACTORY

W. JAMISON DECAY

THIS IS THE DEVOURING MONSTER INVENTED BY TECHNOCRACY

"I am come that they might have life, and that they might have it more abundantly."

THOSE words, from the tenth verse, tenth chapter of St. John, apply to modern machinery. It has come not "to kill and to destroy," but that men may "have life, and that they may have it more ABUNDANTLY."

"Technocracy" is the bugbear that frightens some modern minds, an ingenious invention that lends passing notoriety to a few, the excuse of the feeble.

The greatest blessing of mankind, THE POWER OF MACHINERY, is called by technocracy the cause of all our woes, industrial, financial.

We produce TOO MUCH, therefore, we are unhappy. Men have invented machines that free them from the slavery of pick and shovel, ax and broom, and so they lack work and are hungry.

Nothing could be more preposterous than technocracy's teachings.

that the ghost of her grandmother might reside in one of those flies. She is wrong about that, and technocracy is wrong.

It is your duty to read all that you can on the subject of technocracy. To know and judge FOR YOURSELF is the only way.

Mr. Scott tells you that the United States has installed one thousand million horsepower of machinery, and if all that were operated at full capacity, night and day, "its output would be equivalent to the human labor of over five

TECHNOCRACY IN THE CHANGING TECHNOLOGICAL LANDSCAPE

Technology is developing at an astonishing rate, as evidenced by the booming number of start-ups and the multitude of technological products corporations are developing at an unprecedented pace. The 21st century has presented the governing systems across the world with new issues, like management of digital infrastructure, cybersecurity, maintenance of AI systems and climate technology, each of which demands an advanced understanding of technologies, and could rapidly surpass policies with lack of governmental support.

In this era, technocracy, a system where the rulers are technically skilled experts, came into play to solve problems presented in a rapidly evolving, environmentally concerned and socioeconomic disparity-stricken modern society. Analyzing the contribution of technocracy in present day societies gives us insights into the relationship between technology, knowledge and political power in the creation of policies.

Briefly, "technocracy" is a term used to describe a blend of power and skill, impacting societies through groundbreaking technology development, leading the implementation of tech with formulation of policies, and wielding power.

Ever thought there will be father of technocracy? Thorstein Veblen is recognised as the father of technocracy after publishing an article in 1921- Engineers and the Price System. In 1919, a California engineer, William Henry Smyth introduced this term in his published article “Technocracy-Ways and Means to Gain Industrial Democracy”. Smyth defined it to refer to industry democracy, where engineers and scientists are incorporated in the decision-making through existing firms.

NITI Aayog
National Institution for Transforming India
सत्यमेव जयते

The use of artificial intelligence is also a factor as countries turn to systems to process enormous data sets and reveal correlations in order to aid decision making. For instance, they can analyze current economic forecasts, manage traffic in large urban centers, help organize health initiatives, and identify fraudulent practices in government systems. Another significant advancement being made is the concept of the "smart city".Smart city governance is being actively pursued by nations such as Singapore and have been developed by experts that use systems that will collect real time data to monitor energy consumption, traffic management systems, waste disposal services, etc.

As a result, in order to move into the future, the system of governance will have to maintain the alliance between democracy and expertise, in order for societies to effectively integrate new technological innovations while keeping democratic ideals in focus.

The NITI Aayog, has received technocratic influence because of its data analysis, research and expert knowledge. It is reflected in the policies shaped in digital transformation,artificial ntelligence, sustainable development, and innovation ecosystems.

A technocrat's role is to help governments to comprehend the various dangers of technology and identify alternative opportunities as well as to produce effective and safe regulations. For example, countries like Singapore have implemented technocratic principles through placing skilled individuals at the forefront of managing smart city design, developing e-governance platforms, and initiating advanced technologies.

Not too long ago, it was an established belief that cybersecurity was the sole responsibility of IT, the realm that was often hidden from plain sight. Today, that picture has shifted dramatically, and cybersecurity has transcended its technical confines to become a matter of universal concern, regardless of age or digital literacy.

THE UNIVERSAL THREAT OF SCAMS

We are all in the same boat when it comes to fraud: This realization is not a matter of choice; rather, it has become of pure quantity and guile of present internet fraud and consequently to a person least aware about technology to even the more knowledgeable ones: to everyone who can become well aware of online presence of these scams. You must have also received a fraudulent text message at some point, or an email from someone pretending to be a sender, about some parcel's delivery, or an online scam… all trying to use our flaws as leverage so that we can all be duped by them. What you could lose is everything from your identity, to the money that you have managed to save.
Hence, things like using complex passwords, two step authentication, the need for validating the sender of your emails, etc., are now equivalent to checking and locking the doors of your house. Digital hygiene is gradually but certainly becoming a reflex action.

OVERCOMING THE GENERATION GAP

Although younger generations have grown up online, and acts such as identifying a troll comment or using privacy settings has always part of the day-to-day life for them, what has been surprising is how fast the older generation have adapted to the situation. Years earlier, explaining the dangers of an email phishing scam seemed like a huge task, now those very demographics are the people who often tell you that the WhatsApp message linking to a dodgy URL and calls asking for security code is an OTP scam, or that they suspect it's a customer service scam call.

As life increasingly happens in the digital sphere – whether its transacting money online, shopping, or even keeping up with friends and family – all lives inevitably become exposed in a shared environment. Once your parents have begun offering you tips on protecting your digital self you can confirm it has stopped being a purely technical issue and has become essential for basic survival in this day and age.

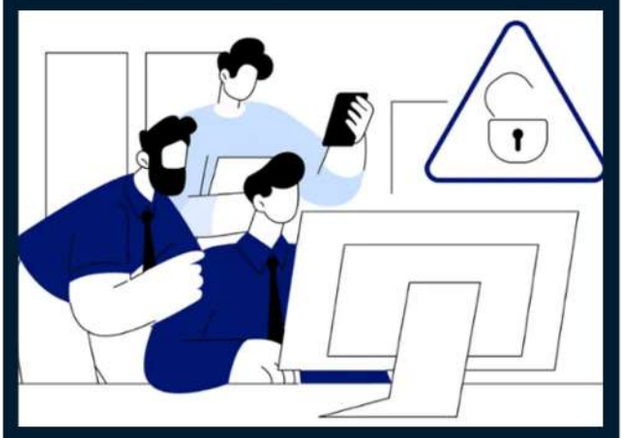
AI, A DOUBLE-EDGED SWORD

In the era of AI, the technology is a treatment as well as a threat for everyone. In the attack domain, generative AI has brought our online fraud more aggressive and dangerous. The fact that it can write a geo, and culture localized phishing email or impersonate the voice of your distressed loved one with deepfake technology has made it even more formidable than ever, and overtime also harder to detect.

Moreover, the increase in efficiency on usage of AI makes cybercriminals achieve more targeted, and faster attack. In defense domain, it is obvious AI will play a part to become an essential in our life. There exist super advanced and efficient security systems where machine learning will analyze gigantic amounts of data to spot abnormality in logging patterns or abnormal financial transactions so that we can detect them prior to the total loss of the money or block their access to the target.

LOOKING FORWARD

This huge shift in human psychology toward digital security is a landmark event for society. We can no longer afford to treat the internet as a benign playground. An understanding of the basics of online security is now uppermost priority for every individual in society, especially in light of the proliferation of AI, and as technology continues to evolve at breakneck speed, collective alertness remains our best defense.



FOUNDATIONS OF CYBER THINKING

We live in an era where our bank accounts, our medical records, and most private conversations exist as data. Now, if I tell you that we don't need a manual to know not to leave our front doors open or hand our wallet to a stranger, we call that smartness. Similarly, in digital world, we call it Cyber Thinking.

People realized that digital security is a survival instinct in this modern world of cloud computing and remote work. The foundation of cyber thinking is based on a simple, disciplined framework of risk, verification, and resilience.

When we think about cybersecurity, it's natural to focus on technical security measures that help protect our digital data. But we are people not AI. The best way to protect ourselves is to foster a proactive, resilient culture of cybersecurity that supports effective risk reduction, incident detection and response, and continuous collaboration.

The cyber security strategy is based on the following three fundamental pillars:

People : This is the human element. It includes everyone from IT staff to end-users. Often seen as weakest link, but can become the strongest defense with proper training and awareness.

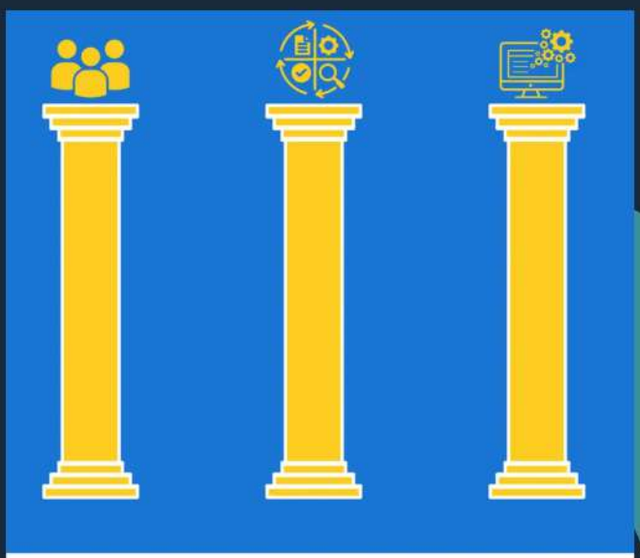
Process : It includes policies, procedures, and protocols that focuses on the management and protection of information

Technology : This combines the tools and solutions used to protect an organisation's digital assets. Technology includes firewalls, antivirus software, encryption, and intrusion detection systems.

Cybersecurity is built on foundational principles that are meant to ensure information remains safe, accurate, and accessible at all times.

The principles also known as CIA triad:
Confidentiality means keeping data a secret from everyone except those who we want to access it.
Integrity ensures that data hasn't become corrupted, tampered with, or altered in an unauthorized manner.
Availability means that data is easily accessible whenever needed for the authorities.

The extended pillars complement the CIA triad, and provide an even better framework for protecting all information assets. These are authenticity and non-Repudiation.



Authenticity is the property that an entity is what it claims to be.

Non-repudiation is defined as the ability to prove the occurrence of a claimed event or action and its originating entities.

Though historically cyber thinking followed the reactive approach but, in modern scenario its more proactive and let to Zero trust Architecture, Least Privilege Access and Defense in depth. Foundation of cyber thinking also surrounds Digital Citizenship which includes the understanding of the legal and ethical online conduct with a calculated approach to data privacy.

Building a Cyber-First Mindset

Cyber Security is popularly known to be an afterthought, something requiring an outside influence, whether that be a cautionary tale, "you know what happened to my uncle's friend's father's coworker's sibling's company?" or a mandated compliance, a pressure of a security audit, etc.
Even then, there exists an air of paranoia around the cyber first architecture. This is beyond the reactive approach of it, cyber security is thought of as layer upon layer of limitations than it is a safety blanket.

From blocking unsafe website, locking things down, banning USBs, people have begun too associate any measure in the workplace with fear.
A cyber-first mindset aims to flip this very ideology, that the act of being secure digitally is proactive, not reactive. That it is baked into decisions right from the get go rather than taking a nail and hammer to a door after it has been broken into.

Following the precedent of cautionary tales, the concept of culture over compliance was introduced. Compliance means rules, ones mandated by a government body, or an authority- these restrict and force an organization into a box of safety. These very guidelines and rules form the first layer of safety for anyone with a digital presence. Concepts like SbD (Secure-by-Design), pushed by CISA (Cybersecurity an Infrastructure Security Agency), the NIST Cybersecurity Framework, etc. form the backbone of cyber-first policy.

But this isn't enough, and mindset must precede policy.

A technocrat is a representative of various multitudes ranging from policy making, regulation, senior government to officials in an institution. They shape the entire ecosystem of any organization which is why it is necessary that none of them treat cyber safety dismissively, because then the entirety is prone to mirror that indifference.

That's where threat intelligence literacy, a widely accepted industry standard model, offers us three layers to understand what the threat landscape from different perspectives.
Rather than every developer, or employee being expected to put on armour and "suit up," prior knowledge of threat intelligence offers that every leader in a digital setting understand enough of what happens to ask the right questions, allocate the right resources, and recognize when things are wrong.

The Tactical layer, is the understanding of common types of attack prevalent nowadays, whereas the Operational layer offers knowledge of how attackers target your specific sector of the industry. Lastly, Strategic is the heavier one, it deals with the geopolitical cyber threats and actors sponsored by the state that often affect infrastructure at a national level. Each of these caters a different audience, offering varying benefits and introducing unexplored angle to protect and/or analyse.

Another take on cyber security, often prevalent is more cautious side of the industry is to build impenetrable walls, and what better analogy to serve the issue here than the tale of Achaean Greeks and their Trojan Horse. Troy built the perfect wall, but it came crumbling down nonetheless.

Much like the moral of the story, the mentioned model of prevention too, is too a victim of creativity. Leaving the only protection, the expectation that something will get in. While that leaves a bitter aftertaste, it is the only strategic IN. The gospel for this approach asks technocrats to build detection than staking everything at prevention. How best can you contain a leak when it happens? How do you recover and fall back? Organizations that skip or deny these questions are known to become history, to be a playbook of what not to do for their successors.

As a technocrat, a cyber first mindset is your anchor in the sea of unrelenting innovation. With a world that moves and evolves so fast that being blindfolded in it doesn't feel much different, we must let the narratives change. Question things, target information, let it shape your response as well as you do your resilience. No wall in history regardless of its height has survived against change, until the wall itself was changed.

Secure-by-Design Mindset

'Prevention is better than cure.'

Software development often mimics the cartoonish action of taping over a leaking bottle. Whenever a crack occurs, another snap of duct tape gets plastered on, over and over, until the software loses originality, and a developer, their mind. While the tactic works to a certain extent, in the long run, such an approach renders the software bloated, and harder to fix.

Secure by Design, or SbD roots from cybersecurity and systems engineering. It enforces a mindset to incorporate security into systems from the outset, instead of as an afterthought. The concept applies on everything from building a product, a service, a system, and down to a consumer's practice of interacting with any of these. It challenges the final phase of deployment practice of adding security at end of development.

Check Point defines the main tenets or the main principles of "Secure-by-Design" as:

- Adoption of robust frameworks and practices in cybersecurity,
- The establishment of string data protection controls, and
- Incorporation of security testing in ALL phases of development.

The Holy Grail of SbD, or the Ten Principles :

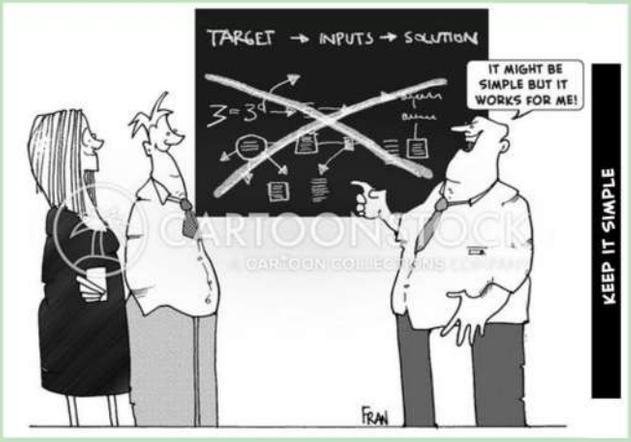
Beginning right off the bat with **Principle of Least Privilege.** It means only giving people access to what they require to be able to do their jobs. Least privilege defines the smallest window possible for any attack, which SbD believes is significantly minimized if each component of the ecosystem (user, process, and systems) operates with the bare minimum permissions required to perform their specific functions.

With security in every endpoint, network, data, application, coupled with identity management, we derive **Defence in Depth**. Rather than handing the kingdom keys to one almighty knight; asking them to guard, protect, defend, we get an army of specialized generals. If the analogy didn't track, it is like securing a house, you get the locks, an alarm system, a fence, a CCTV set, and a trusted bat.

A **Failsafe**, is best described by Murphy's Law,

'Anything and everything that CAN go wrong, WILL go wrong.'

A failsafe is anything and everything from a firewall, a consistent data backup, mechanisms that lock the system down on intrusion. It is however essential to ensure regularly testing, default deny policies whenever and wherever possible, and the automation of recovery processes.



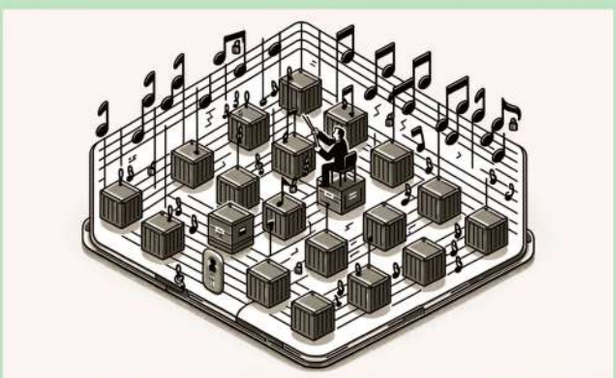
My favorite, **KISS**, aka, **Keep It Simple, Stupid**. More complexity, higher the difficulty in securing it, a double-edged sword really. Complexities ALWAYS introduce vulnerability, and security thrives in simplicity.

Spreading risk, or **Separation of Duties**. Similar to Least Privilege, we don't want a singular person to have too much control, which is why we separate the 'duties.' Example, say in, finance, one takes approving, another auditing, rather than both tasks being under one person.

Open Design, also described as Avoid Security by Obscurity. Keep your security mechanisms a secret, sounds iron-clad, but bad idea. Cryptography defines this with Kirchhoff's principle:

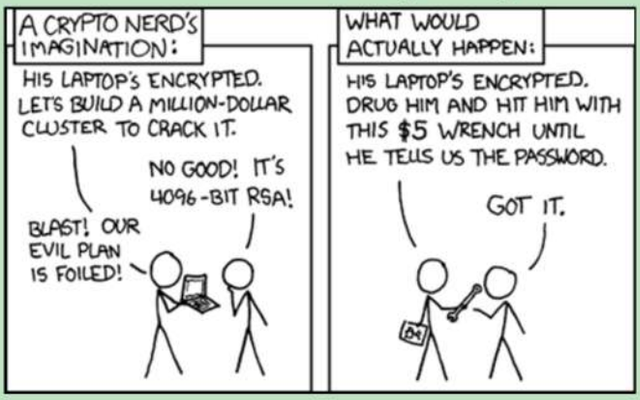
'A cryptosystem should be secure, even if everything about the system, except the key, is public knowledge.'

Or as we choose to interpret it, the secret should be the key, not how the system works.



Others include, **Segmentation**, where we break down the system into isolated components, ideally with firewalls between each unit.

Usability, is more user front, like keep passwords simple enough that user won't forget, but not simple enough that it is '123456.'
It is important to find a balance that remembers that humans are the weakest link in any security chain.



Lastly, we have **Minimize Attack Surface** where we limit external interfaces, restrict all remote access, and reduce components with regular software updates and network segmentation.

And, **Secure by Default**, which just means, implement best practices, prefer restrictive out-of-the-box configurations, and make key considerations your 101.

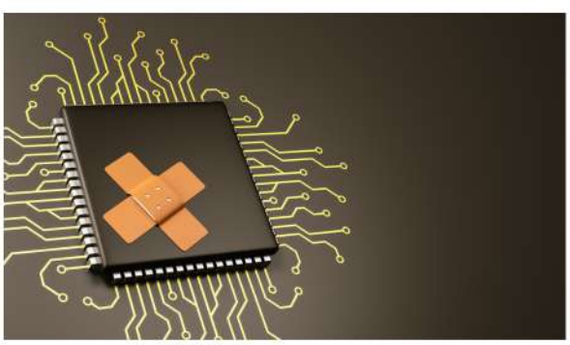
Beyond these, conscious security practices, and awareness of trends and patterns are crucial for any technocrat to be the one shaping cyber security later one day. So, start early, automate, train, and always assume a breach.

PREVENTION OVER PATCH CULTURE

In a world of ever-evolving technology, advancements are what indulged humans to place themselves on a pedestal of worth and glory, yet we feel stagnant in the empty promises; in *dire* need of AGI. The modern software ecosystems not only affect industries with labor, but now threaten our identity, as much as they incentivize not to.

Cybersecurity failures are often perceived as sudden events caused by clever attackers or unexpected technical flaws. In actualization, most breaches are never accidental but the long-term consequences of pre-development stages design decisions itself.

Patching is applying recently-released software updates to fix gap-ups and vulnerabilities, therefore reducing the chances of cyber-exploitation.



Patch culture refers to a reactive security mindset where systems are developed and released quickly, while security is addressed later through updates and fixes.

The logic behind this approach is quite simple: build the product, release it to users, identify vulnerabilities as they appear, patch them, and continue the snake-eating-its-own-tail-cycle.

Patching, the technique, in itself is not inherently problematic; software must evolve, and vulnerabilities will always exist. However, problems arise when patching becomes the primary strategy for security rather than a secondary safeguard.

Most modern software ecosystems rush or postpone security considerations during development and implement design choices that prioritize convenience and speed over digital fortitude. As a result, security gets checked off as a once-in-a-month maintenance activity performed after deployment rather than a principle that guides the design of the system architecture itself.

The formulation of prevention over patching challenges this reactive mindset. Rather, than focusing solely on fixing vulnerabilities after they surface, prevention emphasizes on building systems that reduce the likelihood of their existence in the first place. This approach incorporates practices such as secure-by-design development, least-privilege access control, early threat modeling, rigorous security testing before release, and minimizing unnecessary data storage.

This proves to be extremely crucial as the consequences of cyber incidents(often, not so often) cannot be fully reversed. Patches cannot recover stolen data, restore damaged reputations to their old glory, neither "repair" human trust.

In conclusion, prevention over patching represents a paradigm shift in thinking. Instead of treating security as a corrective action, to be made each time it weakens, it should be treated as an architectural responsibility, shared by all.

Human Error : The Weakest Link

In our society a lot of organizations are spending money on cybersecurity tools. These tools include things like defense systems, firewalls and encryption technologies. They are meant to stop organizations from getting hacked, yet even with these tools cyberattacks still continue to happen.

This is easy to see. The reason is that people are often the weak spot in cybersecurity. Not all cybercrime happens because of machinery failures. It is often mistakes made by people.

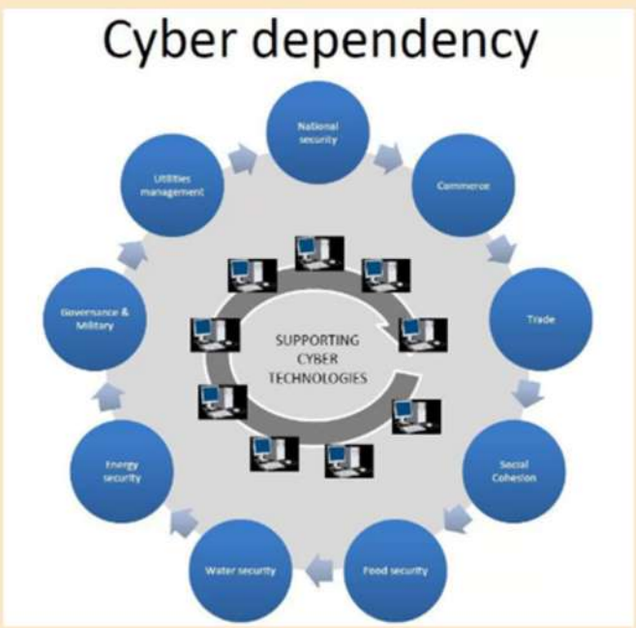
For example, sharing a link or downloading a file can be a big security risk. Using a password or giving out info without checking who they are giving it to can also be a problem. A written phishing email can trick a company with just one click.

Phishing is a problem. Cybercriminals often send emails and messages that look real as if they originate from an actual bank or a coworker. These messages often make the user feel like they have to act, which leads them to act without thinking things through. This can make a user click on links, type in login info or give out info which can let hackers into their organizations' network.

Another big problem is how people manage their cybersecurity passwords. A lot of people use the same password for different things and some use passwords that are easy to guess. So, if one account gets hacked a lot of accounts can be at risk. There is also a risk if you do not update your cybersecurity systems and fix known problems.

The problem of error has gotten worse with Artificial Intelligence. Phishing emails and fake voice calls have gotten very realistic because they use Artificial Intelligence. This has made it harder to know what is real and what is fake.

This does not mean that people are the problem. People need to be aware of these cybersecurity issues. Organizations need to ensure their employees are safe and know how to protect themselves from cyberattacks. This can be done with cybersecurity training and by having cybersecurity security policies.



Cyber safety is just as important as safety. Big risks can be avoided by doing things like checking if a message is real using two-factor authorization and using cybersecurity password management software.

In the end people can be the weak link in cybersecurity but they can also be the strongest if they are aware, trained and careful about cybersecurity.

Cybersecurity is a deal and people need to take it seriously. Organizations need to help their employees understand the cybersecurity risks and how to protect themselves from cyberattacks. This way people can be the link, in cybersecurity.

AI Systems and Cyber Exposure

The internet is something that we use daily to make online payments, use social media, online shopping, online education, entertainment, and professional communication. The more we come into contact with computers, the more vulnerable our information becomes. Today, the concept of AI is something that has become highly widespread in the digital world, affecting cybersecurity protection and cyber risk.

AI systems are becoming more common in industries. Identification of fraudulent transactions is done by banks in real-time using AI-powered algorithms. The use of machine learning algorithms in e-commerce helps in the detection of suspicious buying behaviors. The use of AI in companies that operate on social media helps in the identification of fake accounts, misinformation, and harmful contents. In the cybersecurity operations center, the use of AI helps in the processing of large amounts of data, the identification of something out of the ordinary, and in responding to the detected threats in a more efficient manner compared to the capabilities of humans.

In some cases, the use of AI has improved digital security by improving the speed, accuracy, and predictability of the operations of the cybersecurity operations center.

However, the use of AI is not the sole defensive mechanism for the protection of the digital world, as the use of AI is also done by cybercriminals. Today, the use of AI by hackers is for the creation of highly realistic phishing emails, deepfake videos, voice calls that are cloned and can be easily tricked by anyone, which were previously done by humans. The use of AI-powered automation has made the identification of vulnerabilities in the system easy, which has made the exposure of the sector to cyber threats more common.

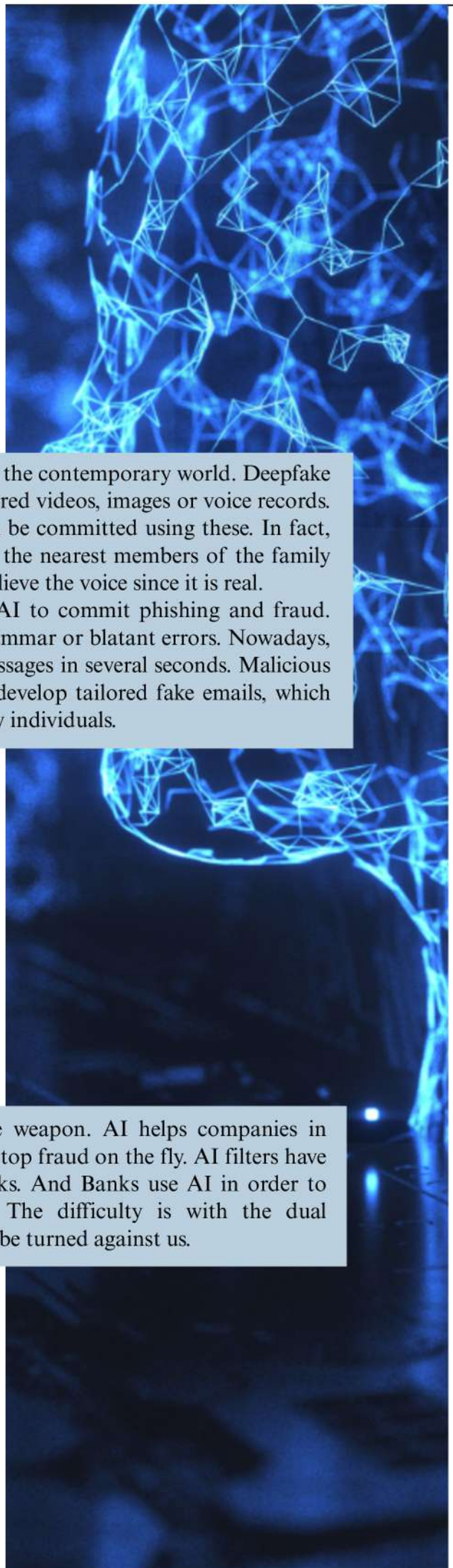
Even AI systems are exposed to cyber-attacks. In cases where cyber attackers do not train the AI model with genuine data, referred to as data poisoning, it is possible for the AI model to produce biased information. In other instances, AI systems lack security, and therefore, it is possible for sensitive information to be leaked unintentionally. In addition, because of the increase in the usage of external AI tools by employees, commonly referred to as shadow AI, it is possible to leak sensitive information unless security measures are put in place.

This, therefore, poses an extremely important question: How safe can we ever feel online? In terms of professionalism, from the perspective of cybersecurity, we can all agree that we cannot feel 100% safe online. This is because safety is an impossibility, especially because technology is constantly changing. Cyber risks will always exist, especially as artificially intelligent systems continue to be developed.

Even though safety is an impossibility, safety reduction is, however, achievable. This is through embracing security measures such as access control, encryption, AI risk management, constant monitoring, security audits, and AI risk management frameworks. At the personal level, it is recommended that we practice digital hygiene, which is explained as the use of robust passwords, two-factor authentication, and being cautious when divulging personal information.

Artificial Intelligence is a two-sided sword. This is because it uplifts our ability to safeguard digital systems, but it has, on the other hand, also empowered cyber attackers.
AI is therefore not something we should shy away from; it should be controlled and made secure.

Everyday AI Threat Landscape



Artificial Intelligence is not a future vision anymore. It is part of our daily lives. Voice assistants and chatbots, online suggestions and online payments are a few of the examples of how AI works behind the scenes of most of our daily services. The convenience and efficiency it tends to introduce has created a new, emerging threat-space that impacts the everyday use.

The AI-generated deepfakes are one of the most noticeable risks in the contemporary world. Deepfake technology involves the utilization of AI to generate realistic doctored videos, images or voice records. Misinformation, ruining reputations, and even financial fraud can be committed using these. In fact, conmen can steal the voice of a person and make a phone call to the nearest members of the family inquiring about an emergency transfer of funds. Victims tend to believe the voice since it is real.
The other more significant issue that is emerging is the use of AI to commit phishing and fraud. Previously, it was easy to detect phishing emails due to the bad grammar or blatant errors. Nowadays, AI can create highly professional, personalized and convincing messages in several seconds. Malicious software developers teach AI to analyse social media courses to develop tailored fake emails, which seem to be genuine. It complicates the process of fraud detection by individuals.

Cyberattacks are also being automated with the help of AI. Through AI, attackers can scan thousands of systems in a short period of time and detect their vulnerabilities and attack them on a massive scale. Even smaller corporations and students have become potential victims. Complications that once had to be done with the assistance of technical skills can be performed now without having special AI tools. Another risk that occurs on a daily basis concerns the manipulation of social media. The AI algorithms are able to make fake accounts, realistic account images, and fake news spread quickly. This has the potential to affect the general sentiment, induce panic, or harm the confidence in online platforms.

Nevertheless, AI is not a threat only. It is also a great defense weapon. AI helps companies in cybersecurity to identify suspicious transactions, block them, and stop fraud on the fly. AI filters have been applied by email providers to filter spam and malicious links. And Banks use AI in order to track transactions and warn users about suspicious activity. The difficulty is with the dual dispensation of AI. It is the technology that protects us that might be turned against us.

That is why how are we going to be safe in this every-day AI threat environment? Originally, never believe the calls or messages which seem authentic but are unexpected. Second, do not publish sensitive personal information on the Internet. Third, account enable two-factor authentication of critical accounts. Lastly, keep running with the threats coming up in the digital world. The implementation of Artificial Intelligence is changing our world in an unbelievable rate. Awareness and responsible actions on our digital front are our best weapons.

Author : Anushree

Digital Footprints & Identity

In today's digital world, our lives are associated with the online world to a great extent. Every single action we perform in there leaves a mark

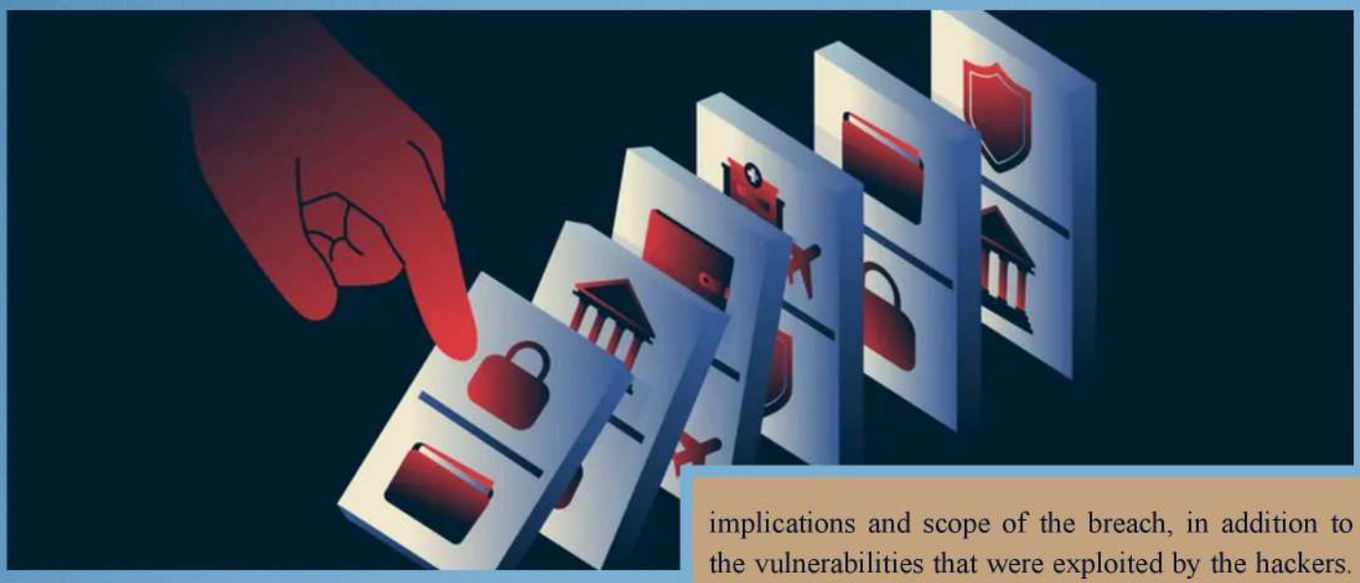
and a footprint. Whether it is creating a social media profile or an online shopping experience. Our footprint and how it influences our online identity is an important part of our digital experience. It has been seen that we are unaware of the fact that every single activity we perform in the online world leaves a small trace of information behind. Such small traces of information are only known as digital footprints. This is a term that is used for "a set of data that is created when a person uses the internet." With time, all these digital footprints combine to form a digital identity that defines how a person looks in the online world.

These footprints can be of two types: active and passive. Active footprints include the information we willingly provide, such as on social media sites or while filling out online forms. On the other hand, Passive foot printing includes the gathering of information without our direct knowledge, such as when websites record our online history with the help of cookies, or even if our IP address is recorded. This information can be used to create a profile of our interests, habits, and even geographical location, which can be used by advertisers, marketers, employers, and even educational institutions.

The consequences of digital footprints could be wide-ranging. The consequences could be wide-ranging and could even extend to our lives as individuals, and even to our professional lives, it could even extend to our reputation, the chances of getting a good job, and even to our relationships, for instance, a careless remark could be misinterpreted, which could lead to damage to reputation. Too much information could be shared on the social media sites, which could lead to identity theft scams. We should be conscious of the information we share and the people we share it with. The privacy of the information we share on the various social media sites should be reviewed to determine who can see the information we share. Think before you post.

Digital footprints and digital identity have come to be the two faces of the same coin in the digital age. Every one of our digital activities has come to contribute to the "mosaic" that is us, both from our own point of view and from the point of view of others. While digital footprints have come to offer us opportunities and insights that are valuable to us, it has also come to demand that we be vigilant in our digital activities in the name of privacy and reputation. The awareness of one's digital footprint is very essential in the maintenance of a secure, authentic, and respected digital identity.

The Cost of Cyber Negligence



In the present digital world, the internet has become an integral part of our lives. People depend on technology for their studies, communicating, online shopping, online transactions, and entertainment. Likewise, organizations have come to depend on technology for storing their data and conducting their business. Though technology has simplified and eased our lives, it has also raised the stakes for cyber security. Unfortunately, many people and organizations fail to take adequate measures to secure their online data. This lack of concern for cyber security is called cyber negligence.

Cyber negligence can be defined, as the negligence or failure of an individual or organization to protect their digital assets with reasonable care leading to a breach in security of the digital asset. Cyber negligence can be described as having grave consequences, not just for people whose data is compromised in a breach, but for the economy as a whole. The cost of cyber negligence is also of critical importance in enforcing the individuals, organizations, and countries to take necessary measures while governing cyber security.

The financial costs of cyber negligence are substantial. As a consequence, data breach may lead to considerable costs, including legal and regulatory costs. In other instances, it may require an organization to invest heavily in making sense of the data breach in order to understand the implications and scope of the breach, in addition to the vulnerabilities that were exploited by the hackers. Moreover, it may cause a business to lose its customers and sales due to damage to its reputation. The costs of downtime, in which an organization may be unable to carry on with its activities due to a data breach, may be considerable, especially in businesses that depend on digital infrastructure. The cost of cyber negligence may be between millions and billions of dollars depending on the extent of data breach.

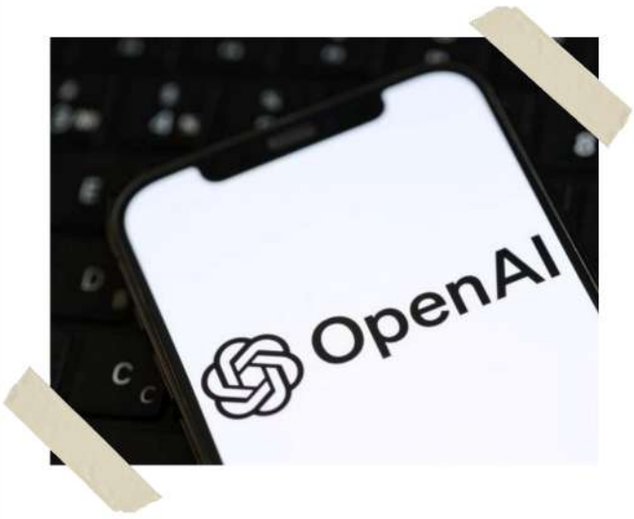
Apart from financial losses, data breaches due to cyber negligence may also lead to damage to the company's reputation. A data security breach may damage the trust between the company and its stakeholders or customers. The publicity and media attention due to the data security breach may damage the company's brand image, thereby affecting sales and market.

For example, the Panera Bread restaurant chain faced a cyber-attack in 2026 that significantly impacted the organization. The attackers gained access to a large database of 5.1 million customers' information. The leaked information included the customers' names, email addresses, phone numbers, as well as home addresses. Although the attackers did not access the customers' financial information, experts argue that the leaked information could be used for phishing attacks. Rebuilding trust after a data security breach is a tedious and costly affair that involves investing in marketing strategies.

Author : Anshita

MIXPANEL VENDOR HACK

On the 8th of November 2025, Mixpanel identified an SMS-phishing campaign that led to unauthorised access of and data leak for multiple organisations dependent on the web analytics services provided by them. The organisations known to be affected by the data leak were OpenAI and CoinTracker. While several headlines aimed a sensational approach towards the issue and fear-mongered all ChatGPT users, the affected users were specifically people who had used OpenAI API, were logged into platform.openai.com, or had submitted help center tickets and the leaked data was not particularly sensitive. Mixpanel and OpenAI released statements regarding the security incident within two days from each other.



WHAT WENT WRONG?

The analytics company, self described as an AI powered data clarity platform, suffered an SMS Phishing attack, which they described as a "Smishing Campaign" in their public statement.

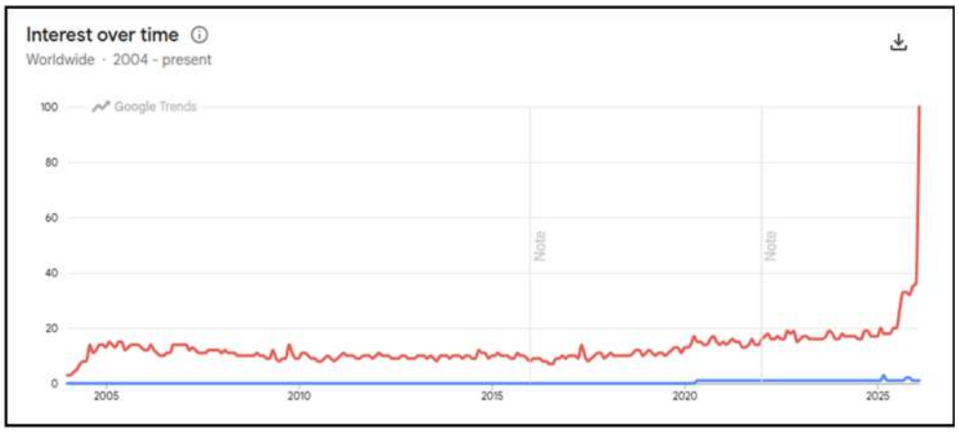


Figure: Google Trends Graph: Red - Phishing Blue – Smishing

In other words, the credentials of a Mixpanel employee were compromised. The attacker used these credentials to access Mixpanel's client data and obtained personally identifiable details such as name, email address, rough location, operating system, browser details, etc. Such information serves as very low leverage ransom data, however, names, email addresses and location can be used to make personalised and targeted phishing campaigns.

THE REMEDIAL MEASURES

Within its statement to the general public, Mixpanel included a list of actions they took to ensure such an incident never occurs again. The ones that were the most substantial were:

- Secured affected accounts
- Revoked all active sessions and sign-ins
- Rotated Credentials
- Engaged third party forensics firm for advise and review
- Implemented additional controls to detect and block similar activity

BREACH VS. LEAK

A factor of the incident that deserved to have more light shed on it was the terminology used to refer to it. Organisational statements called it a data breach. However, public discourse points to the fact that the data was leaked as the unauthorized access was a Mixpanel staff account. Exemplified by Hacker News user kevcampb's analogy of "If someone phishes your Gmail account, there is no Gmail breach.".

THE CONSEQUENCES

Despite the measures and the assurances by Mixpanel, OpenAI terminated their operation with them.

Mixpanel released their public statement regarding the issue on 27th of November 2025 and had informed OpenAI prior to that, and provided the affected dataset on 25th of November 2025. GDPR requires organisations to report data leaks without undue delay. Whether the 19 day time period constitutes an undue delay may be up for interpretation due to the lack of transparency regarding the specifics of the data that was exposed and the companies affected.

Mixpanel's statement was publicly regarded as objectionable at best, specifically due to its use of ex-gratia language, a form of compensation without liability. It deferred from any direct apology to the clients and provided minimal details about the consequences of the leak. OpenAI's article regarding the leak was surprisingly more informative and direct. However, it should be noted that Cointracker sent a suspiciously similarly worded email 3 hours earlier, which can mean that OpenAI either adapted from their template, or they both shared the same template, signifying the approach these organisations have regarding the data of their clients.

Author : Druhi Mehra

ESCAPING THE CYBER MYTHS

With cyber security being the star of the show and a career prospect for many, there's no doubt there are several myths surrounding the field. Most of the myths originate from the representation people working in security research get in the entertainment industry. The other biggest contender for the origins of such myths are people's approach towards cyber security in general.

To commence with, a really common trope in movies is an exciting sequence of someone using CLI tools and loading bars to hack into systems. Whilst most people with even a remotely accurate understanding of the terminal know it is a massive exaggeration, it still manages to allure several people who, upon the realization that cyber security and

penetration testing is a lot less running the right tools pointed at the right target and more log analysis, false positive removal, access and flow control, and the house of cards that is a setup involving several people on different levels of the organizational structure, may lose the motivation and as a result, the precious time and resources along the process.

On the note of the organizational structure, those bitten once by the horrors of bureaucracy in a typical IT firm such as one responsible with web development and container management often fall for the ideal that the field of cyber security can allow them a lifestyle devoid of dependence on other people with different capabilities. The security measures, regulations, and policies for organizations are set up by a group of people.

When proper documentation is traded for reliance on individuals. More often than not, breach resolution is bottlenecked less by one's own understanding of the process and more by the wait for a response from some sysadmin who left the organization years ago and knows the credentials required. Whenever a new innovation comes along, it is hyped by claims of replacement of some or other section of the workforce.

The Matrix [1999]

This is one of the easiest ways innovations achieve funding targets as the priority for most investors and executives is to reduce spending on employees and the anti-exploitation regulations that are accompanied with the human labor cost. For cybersecurity, the antagonists of the myth have been behavior analysis, then NGAV (next-generation antivirus), and presently Gen-AI.

Evidently, the argument is canard as the context limitations of Gen-AI render it suitable only for low-reference work such as creation of unit-tests, semantic searches or second passes through documentations, etc.

To conclude, cyber security is an exciting field, but not in the ways seen in media tropes. It still involves social interactions and references beyond documentations and can not fulfil the desire of independent planning and execution, but human interaction and lost sleep over vulnerabilities is a key part of the excitement. The substitution of human labor in the domain, like most technical divisions, is still beyond the capabilities of generative AI and NLP.

CYBER PSYCHOLOGY *and* HUMAN BEHAVIOUR

In the modern digital world, the internet and technology are a part of our lives. People use smartphones, computers, and the internet for studying, communicating, shopping, and entertaining themselves, and even working. As people are spending more and more time in the virtual world, it is also important to analyse the impact of the virtual world on the thought process, feelings, and behaviour of people. The branch of psychology that analyses the impact of technology on the behaviour of people is known as cyber psychology.

Cyber psychology is the study of how people relate with technology. In this field of study, the focus is on how people relate with technology and how this affects their emotions, decisions, and behaviour. When people relate with technology through communication using social media, emails, online games, or messages, their behaviour can differ from how they react in real-world scenarios. This is so because the cyber world offers people a different environment where people are not present.

One of the important factors of cyber psychology is how social media affects our mental health. Facebook, Instagram, Twitter, etc., are an essential part of our lives. However, as seen in all other things in life, the use of social media also has two sides: a good side and a bad side. Excessive use of social media is associated with a high level of anxiety disorders, depression, and issues of body image.

Social media has made us social comparators. Everyone is trying to show off their perfect life on social media. We all compare ourselves to others, resulting in low self-esteem and feelings of inadequacy. We have become victims of information overload. Information overload is resulting in anxiety. We are in an era where we have to be "on."
Another interesting aspect explored by cyber psychology is the online disinhibition effect. This refers to a situation whereby an individual may feel that they're unrestricted when are communicating online. This is because they are not physically present and can feel a certain level of anonymity. This can, therefore, enable individuals to speak more freely and express themselves more than they could under normal circumstances. This can be both negative and positive depending on the circumstances. It can enable individuals to share their feelings and can also cause negative behaviours such as cyberbullying.

Cyber psychology also provides us with interesting insights into the role of technology in influencing our thinking, feeling, and behaving patterns. It also points out the advantages as well as the disadvantages of the digital age that we live in, enabling us to come up with strategies to effectively utilize technology in a positive manner to enhance our mental well-being in the cyber world by being aware of our usage of social media, practicing good communication skills in the online world, and seeking assistance if we face problems in the online world.

Author : Anshita

BYBIT CRYPTO HEIST

It feels fundamentally wrong to be delving into the world of cybersecurity and have no mention of cryptocurrency. After all, the biggest concern when it comes to the territory of scams and frauds, till date, remains money.

The biggest heist in world history was a crown that for over decades now, had proudly adorned the head of Central Bank of Iraq and its infamous 2003 debacle, where nearly a billion dollars in cash was taken by a mere handwritten note by Saddam Hussein's son, Qusay Hussein. What we must emphasize here, is the past tense of the sentence, and the quietly slipped indication that the crown has found a new home. The Bybit Crypto Heist reads like a movie, but unfortunately bears the classification of a documentary. And it began with a singular developer. This, dear reader, is where I would say to buckle-in.

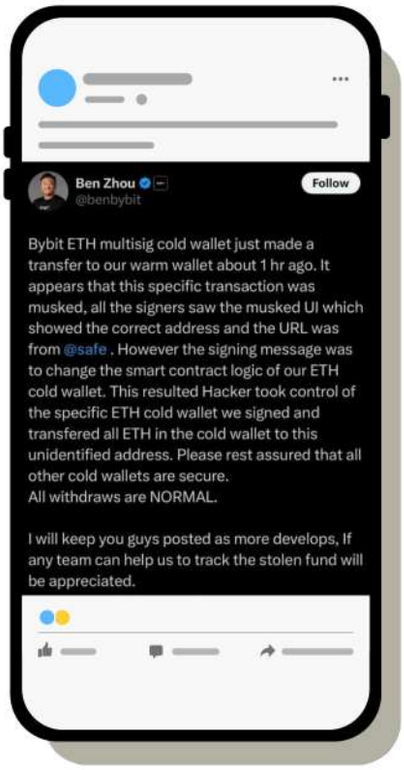
We begin right at the heart of the organization, the headquarters of Bybit. On 21st February, 2025 per routine procedures, Bybit had been conducting a transfer of Ethereum from cold to warm storage, a measure that aims to store the cryptocurrencies in order to prevent hacking. Over 4,01,346 ETH funds began to undergo the transfer, but the speed was unusually dull for what the activity usually took. A developer's instinct, of course, is not too panic, but groan at a the likelihood of it being a bug, the thought of a potential, highly sophisticated attack, a buried afterthought that wasn't due to strike yet.
Until, of course, it was found that the funds were not 'stuck' but had instead been intercepted.

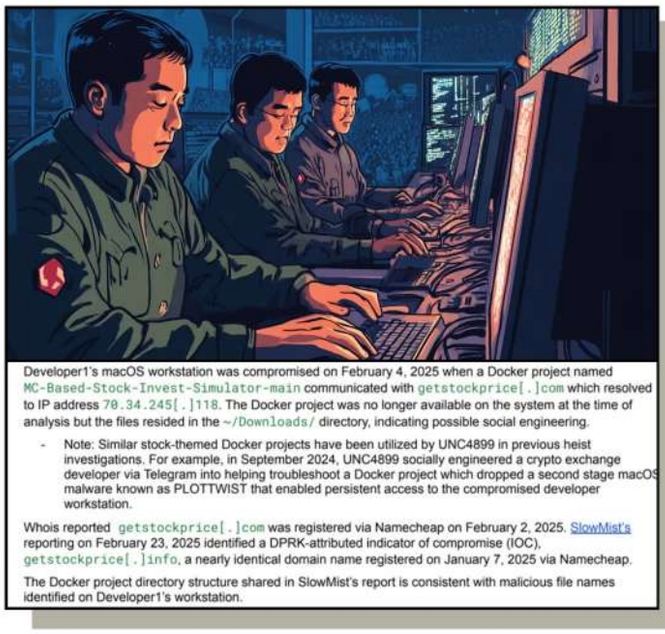
While the issue got flagged in late February; after it was already too late, the heist had actually begun multiple weeks prior. The alleged culprit and perpetrator of the incident, and the organization that Bybit has sworn to wage a war against, is Lazarus.

Lazarus is an infamous North Korean criminal hacking group that earned its fame from some notable hacks over history, including but not limited to the Sony Pictures hack of 2014. The only question here now, is how they get in, in the first place. Of the most common tactics the group employs, that also marked their 'IN' was to pose as recruiter.

A South Korean, Rust Developer from a partner company Safe, became the scapegoat. The 28-year-old developer received a job offer that marked the checkboxes on every developer's dream that they begin envisioning day-1 of their college life.

Deeming the outreach legitimate, he began communication with one of the highest sophisticated hacker groups to exist. As an assessment test, the developer was delivered a huge codebase which we now know hid a malware of sorts.
Over the span of time from its execution, till the 21st of February, AWS session token were stolen, multi-factor authentication was bypassed, and Lazarus slowly but surely slid into Safe {Wallet}'s interface, leading to the events we discussed earlier.





Developer1's macOS workstation was compromised on February 4, 2025 when a Docker project named `MC-Based-Stock-Invest-Simulator-main` communicated with `getstockprice[.]com` which resolved to IP address `70.34.245[.]118`. The Docker project was no longer available on the system at the time of analysis but the files resided in the `~/Downloads/` directory, indicating possible social engineering.

- Note: Similar stock-themed Docker projects have been utilized by UNC4899 in previous heist investigations. For example, in September 2024, UNC4899 socially engineered a crypto exchange developer via Telegram into helping troubleshoot a Docker project which dropped a second stage macOS malware known as PLOTTWIST that enabled persistent access to the compromised developer workstation.

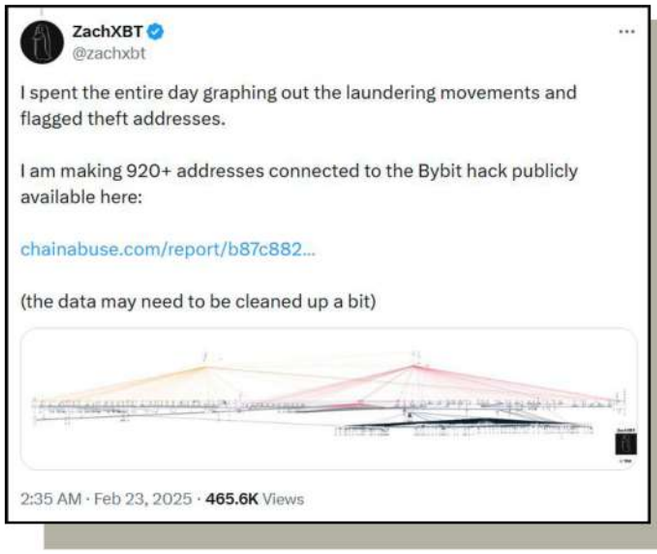
Whois reported `getstockprice[.]com` was registered via Namecheap on February 2, 2025. SlowMist's reporting on February 23, 2025 identified a DPRK-attributed indicator of compromise (IOC), `getstockprice[.]info`, a nearly identical domain name registered on January 7, 2025 via Namecheap.

The Docker project directory structure shared in SlowMist's report is consistent with malicious file names identified on Developer1's workstation.

The heist wasn't as simple as pulling a bag of ETH and stashing it away where the cops can't find. Funds such as these need to be moved. A lot. They were dispersed and swapped quickly over wallets and decentralized exchanges. Through so many services that a trail was near impossible to hash out at that moment. In a matter of hours, hundreds of millions of dollars had been laundered into forms that could neither be frozen nor traced.

It was not until later that investigators traced the compromise to Safe, and a very confused South Korean who had no idea what was happening.

Following Bybit's Lazarus Bounty programs, X user, ZachXBT graphed and flagged each individual theft address, spanning almost thousand addresses.



ZachXBT
@zachxbt

I spent the entire day graphing out the laundering movements and flagged theft addresses.

I am making 920+ addresses connected to the Bybit hack publicly available here:

chainabuse.com/report/b87c882...

(the data may need to be cleaned up a bit)

2:35 AM · Feb 23, 2025 · **465.6K** Views

While the incident raised a multitude of questions, it also redefined how crypto crisis, particularly heists, have been handled over time. The moment the issue got flagged, Ben Zhou, in a matter of hours took to X.com to address the matter, and kept the public in the loop, doing a LIVE, and actively responding on the social media platform. Beyond this, Bybit declared all losses recoverable by investor loans. The platform also, all but withheld, unflinching through four billion dollar withdrawals and then deposits.

Given the long history of poorly handled crypto crisis that have brought down so many companies, Bybit represents a masterclass on how to deal with incidents, and survive.
Investing.com also verified Bybit's 31st proof-of-Reserves Report back in early March, showing that the organization continues to stand strong, maintaining its reserves that either meet or exceed the total user holdings across all of the reported assets.

Ben Zhou
@benbybit

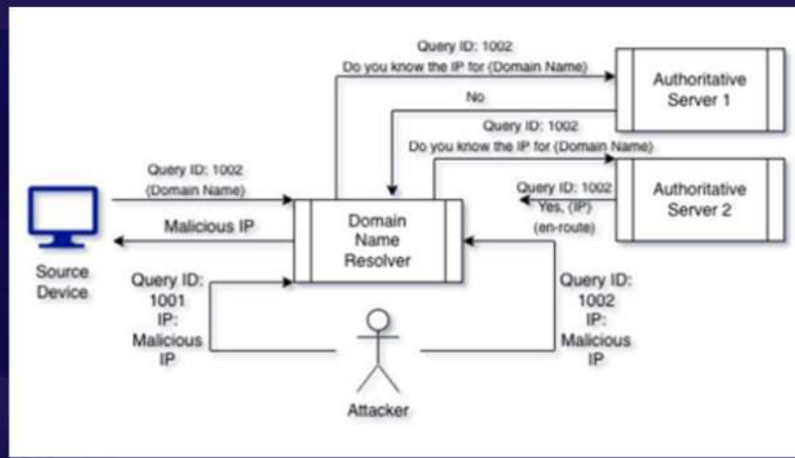
12 hr from the worst hack in history. ALL withdraws have been processed. Our withdraw system is now fully back to normal pace, you can withdraw any amount and experience no delays. Thanks for your patience and we are sorry that this has happened.
Bybit will come out with full incident report as well as security measurement in the next few days. I will also personally keep you all posted on any new updates. Thanks to all the clients, friends and partners who have helped and supported us during this excruciation 12 hrs.
The real work has just now started.

3:51 AM · Feb 22, 2025 · **3.1M** Views

THE WONDERS OF DNS POISONING

The concerns regarding cybersecurity are ever decreasing amongst lay-people with technological innovations. It's not a consequence of reduced risk of cyber-attacks as much as it is the mainstream expectation of outsourced risk aversion. People expect the operating systems, software, and websites (or SaaS applications) they use to implement security measures and account for their actions. As a developer, it is one of the implicit responsibilities to make intuitive and safe experiences, prompting users about actions that they may not intend, such as deletion of root directories, downloading content or sending sensitive information through http protocol, and other such actions. Good development practices reinforce users' trust in the services and consequently alleviate their concern about cybersecurity.

This article aims to provide a historic overview of a problem that exploited said lay-people and how improvements in the pillars of the internet and the blood and sweat of security researchers went into making the internet a safer place for them. DNS cache poisoning was a form of cyberattack that took advantage of a number of inherent vulnerabilities of DNS. Similar to BGP (not to be confused with another homophonic security risk), DNS was built for a much smaller Internet and based on a principle of trust.

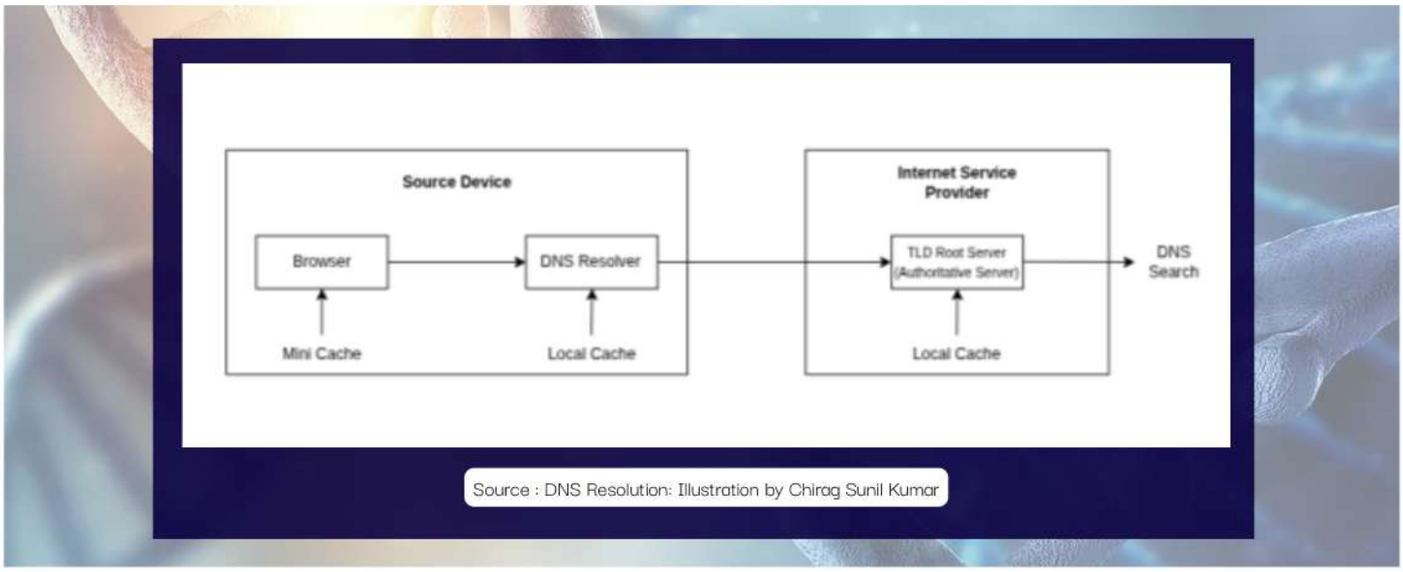


Source : DNS Poisoning: Illustration by Chirag Sunil Kumar

Attackers aim to poison the DNS caches held by domain name resolvers. Incorrect entry in the cache means malicious redirection to users accessing the web addresses for thefirst time. The way typical web searches work is that a device sends a query for an easy-to-memorize domain name (such as lms.jimsipu.org) with a query ID to a domain name resolver, who will look for the IP address for said domain name in its own cache, and ask one "authoritative server" after another if it does not contain the address within its cache. The multi-hop step of asking authoritative servers takes a few milliseconds, giving an attacker nameserver time to spam the resolver with guessed query IDs with a destination IP for a malicious server. The process of guessing query ID's was easier than one would imagine; query IDs were incremental. That meant sniffing the queries from a device for a while and then spamming the next 20-302 query id's to the resolver acting as if our address is the real one would usually do the trick.

The malicious route would stay in the resolver'scache until eithermanually removed, which is rare, or the time to live (TTL), defined by the attacker, expires. To resolve a risk as severe as this, the first obvious change made was to randomize the query ID, leading to 216 possible combinations, and later randomizing the source IPs to another 216 combinations, leading to hundreds of millions of possible permutations of pretty problematic to probe queries.

To conclude, the issue with increasing permutations is that it's only waiting for access to enough compute. The deterministic solution to the issue was the introduction of DNSSEC, an approach which adds signatures to the DNS records, which can be matched to authenticate the nameservers and weed out attacker responses for good.



WHAT BREACHES TEACH TECHNOCRATS

In today's digital world, in case of any breach, it's no longer just an IT issue but rather a golden opportunity for all technology leaders to learn something out of it. The key learning out of all the recent high-profile breaches in the last few years has been that security is a process, not a product. We invest tremendous amounts in getting sophisticated firewalls and best-of-breed security products implemented in our environment, but at times, what seems to have happened in all these breach cases is that security essentially boils down to addressing the weakest link in any given situation.

As a tech expert, reflecting on the consequences of a cyber attack is like getting the blueprints for the next revolutionary breakthrough that will change the world we live in. It is obvious that we are no longer doing things the old way, and we are now employing a new model, or a new paradigm, known as Zero Trust. It is obvious that if the external perimeter is breached, the internal environment is a tempting target. Outside of the defence playbook, these attacks demonstrate that when things go wrong, a good defence is not enough. A swift local response is needed to stop damage from spiraling completely out of control.

By studying what happened, technocrats move from reacting to trying to react better in the future. They also learn that openness can win trust and that a brand is not defined by how much data was stolen but how you respond to a crisis. A truly cyber-ready leader is one that is able to pivot when things go wrong and keep systems down for as short a period as possible.

At the end of the day, people are still the weakest link in digital security. Whether through social engineering or password stuffing, people are still the biggest threat to tech leaders who understand that technology is only half the battle. True security is achieved when you change the culture so that everyone in an organization, from intern to CEO, understands that they are a key player in keeping the organization secure. We've learned a lot from the breaches of the last ten years, and each one makes us a bit smarter.

Apart from money and legal issues that may come with any breach of contract, there is a clear signal that points to the need for data hygiene. The technocrats know that data can be as much a liability as it can be an asset. The organization can largely minimize risks if it adopts stringent data retention policies and ensures all its data is encrypted. It also means that if there was to be any breach, the attackers would not be able to access any useful information.

Author : Aditya Pratap Singh

BRIDGING THE CYBER SKILL-GAP

The process of digital transformation is occurring globally at an incredibly rapid pace. This has created one of the biggest paradoxes in the world today: technology is advancing at a pace that our ability to protect it cannot keep up with. This may be one of the largest skill gaps in today's business world. It's not just a technology issue; it's not just a hiring issue. It's how we think about it.

The old notion of assessing a candidate based on their four-year degree is no longer applicable in today's fast-paced environment. Threats are rising faster than educational institutions can adapt to them, and before a student can graduate, the field changes. Therefore, a new breed of innovative companies is looking to a skill-based model for hiring and training. This provides a new model for a diverse and inclusive technocracy based on skills such as analysis and network forensics.

However, the key piece that was left out was **experiential learning**. *One can know all sorts of things, but one can only really learn something by doing it.* The addition of Capture the Flag (CTF) simulations allows students to develop useful skills to protect themselves. The gamification of learning allows students to be forward-thinking and anticipate how the attacker would react in any given situation. This is a big departure from the "check the boxes" mentality.

Cyberspace security should be an integral part of one's job, and all should own up to it in their workplace. Many times, lack of knowledge arises when security is limited to a few people's understanding. This can be resolved by tech experts initiating a "Security Champions" initiative, where they encourage members from other departments to be the primary security defenders in their teams. In other words, it's all about security knowledge distribution to many people.

This mentorship is out there, but it's on the sidelines and not fully part of the process yet. Expertise can both hinder and help in defining how well the line is drawn between the veteran architect and how well they share that knowledge with the young analyst. Sharing that knowledge is key so that threat hunting and risk management details don't get lost in translation. A culture that encourages curiosity and views failure as a learning tool is the base on which a long-term solution can be built to attract the best talent.

We need a combination of technical skills and emotional intelligence. It is no longer sufficient to train good programmers, we need to develop leaders who are familiar with the emotional, business, and cyber worlds, and all these worlds connect somehow. As threats become more sophisticated, people are still our best defence, relying on our intuition and sense of right and wrong.

Author : Aditya Pratap Singh

MILITARY AI *and* ETHICAL BOUNDARIES

In early 2026, an ethical fight broke out between the Pentagon and AI startup Anthropic. It started because the military demanded for "any lawful use" of AI models, which Anthropic resisted to prevent the technology from being used for mass domestic surveillance and fully autonomous weapons. This resulted in the Trump administration blacklisting Anthropic as a "supply chain risk", reigniting the debate over who controls the ethics of national security technology.

This case study raises at least three critical questions: who should have control over how AI is used in a democratic society? How should that control be exercised? What should the consequences be for a company that disagrees with the government's policy?

Anthropic entered the DoD's ecosystem in late 2024 through a partnership with software and services provider Palantir. Months after that agreement, Claude became the first major model deployed in the government's classified networks through a $200 million contract with the DoD. The model's popularity continued to soar across the business world, particularly in the area of coding assistants. The Defense Secretary. Pete Hegseth also took to X (formely Twitter) and declared that any contractor or supplier doing business with the United States Military is barred from commercial activity with Anthropic.

Following the Trump administration's decision to blacklist Anthropic and designate its technology as a national supply chain risk, defense technology companies and organizations are now telling their employees to stop using Claude, and to switch to other artificial intelligence models and assistants.
It's a sudden reversal for Anthropic, which gets about 80% of its revenue from enterprise customers.

The announcement came after Anthropic executives refused to comply with the government's demands over its model use. They wanted assurances that their AI would not be tapped for fully autonomous weapons or mass domestic surveillance of Americans as it is incompatible with the democratic values.
Though all of this is mostly been limited to social media posts. But multiple defense tech executives said they're preemptively moving their workforce off of Claude.

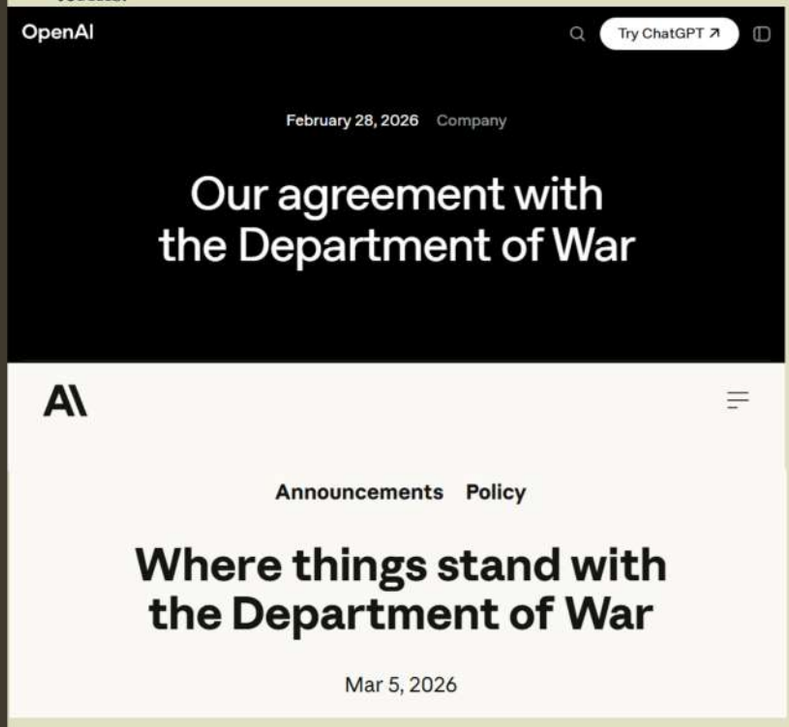
After the announcement by Pentagon, the CEO of OpenAI Sam Altman was swift to capitalize on this friction. The recently turned for-profit organization signed a deal with Pentagon that allows the military to use OpenAI's AI models "for any lawful purpose" as deemed fit by the using authority.

After facing a barrage of criticism, Altman admitted the deal was "sloppy," later he added the company would amend the contract to explicitly prohibit the use of OpenAI's technology for domestic surveillance of Americans.

President Donald Trump also mandated that the federal agencies will have exactly six months to phase out their use of this technology.

So it's not surprising that some people may now have more faith in a seemingly well-intentioned and brilliant, but unelected, technology executive, such as Anthropic's Dario Amodei, to do the right thing and set the right policies.

This lack of legislative clarity has paved the way for "Soft nationalization". The Pentagon's current approach comes close to nationalization by other means. One option the DoD threatened was using the Defense Production Act, a Cold War-era law, to compel Anthropic to deliver an AI model on its preferred terms-a sort of soft nationalization of Anthropic's production pipeline. And the retaliatory decision to label Anthropic a "supply chain risk" is designed in part to intimidate the rest of the industry into accepting the Pentagon's terms.



The crux of this standoff the Pentagon vs Anthropic when the government demands "any lawful use," is a move toward nationalization-adjacent control. It's a way to grab the power of private tech while dodging the need for new laws.

If the US government continues using flimsy legal justifications to punish corporate companies, the boundary between national security and state-run surveillance will disappear. This fight with Anthropic is a huge warning sign that without urgent actions taken by the congress to set clear ethical boundaries, the military will continue to weaponize these legal loopholes. Instead of AI used for democratic defense it will become a tool for domestic intimidation.

Author : Meenakshi Singh [BCA, 3rd Year, Shift-1]

The Google Vishing Breach

On August 8, 2025, Google announced in a blog post that they suffered a data breach, due to an earlier attack on their Corporate Salesforce CRM (Customer Relationship Management System),this may not have been expected since they are often considered one of the most secure companies around the world,proof that even the most well-resourced organizations are not invincible.

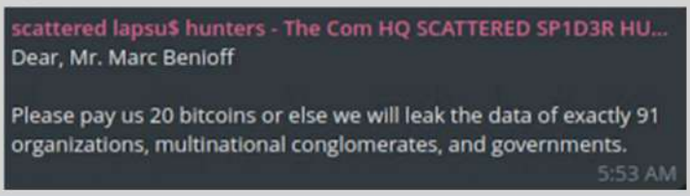
The breach was a result of an attack by the hacker's group ShinyHunters (also known as UNC6040) targeting Google's Salesforce account to gather data about SMB customers (and potential customers) for Google Ad. Google confirmed this data breach on August 8, 2025, which actually happened in June 2025 , after completing their investigation and impact assessment, and notifying those affected.

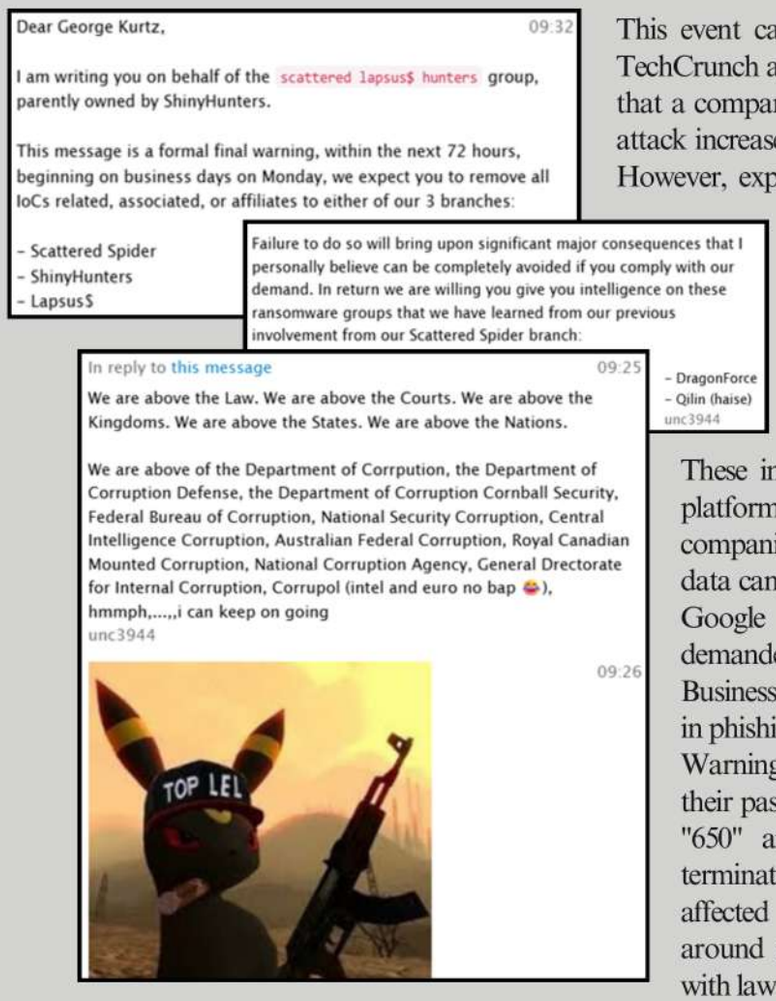
What did ShinyHunters do?

The group of hackers referred to as ShinyHunters (also referred to as UNC6040), specifically intruded into Google's CRMS to collect data on small and medium-sized businesses who were or would have been customers of Google Ads. After completing their analysis, including quantifying the damages of the breach, notifying all impacted individuals and confirming the breach on August 8, 2025, Google reported that the attackers obtained a total of 2,550,000 records containing business names, business telephone numbers and sales rep notes including many pieces of information that may be publicly available, it still holds substantial value to a hacker who wants to use that information to engage in phishing schemes or obtain a competitive advantage. The good news is that no private customer information or payment information was stolen or compromised as part of the breach; therefore, there was no adverse effect on the core operations of Google Ads or Google Analytics.

What was their method of operation?

This incident demonstrates how the majority of today's attackers use social engineering techniques instead of coding in order to commit crimes.They did not use any sophisticated software, they utilized phone phishing known as "vishing" (which is short for voice phishing). ShinyHunters called into Google and impersonated members of IT support, convincing Google employees to authorize a connected app installation, which is a modified version of Salesforce's Data Loader. ShinyHunters thus misled the system and obtained unauthorized access to Google's CRM records. After gaining access, ShinyHunters exported the records before Google could detect the breach and disable their access. According to ShinyHunters, this attack against Google was only one part of a much larger coordinated effort directed at Salesforce Integration's entire customer base. Since the attackers used only social engineering rather than computer-based methods, all standard defenses (firewall technology), which would have been necessary if they had hacked into the environment by changing codes, were completely bypassed, and there were no zero-day exploits or malware used.





This event caused a huge media stir with major outlets such as TechCrunch and Forbes covering the breach in detail. The revelation that a company as large as Google could fall victim to this kind of attack increased already existing debates about security in the cloud. However, experts in the cybersecurity field were quick to point out that this was not a high-tech hack, rather it was an example of social engineering and showed the need for employee training on cyber awareness. Google believed *ShinyHunters* may be preparing to post the stolen data on a data leak site, as the group has been linked to a no. of recent attacks.

These include attacks on Cisco, Qantas, and Pandora,These platforms are used to publish stolen data and pressure companies into paying ransom. Even seemingly harmless basic data can be leveraged for targeted follow-up attacks. However, Google confirmed that the ShinyHunters group never demanded a ransom.

Businesses that were affected by this breach will face an increase in phishing emails that will appear to be authentic from Google. Warnings have been sent to all 2.5 billion Gmail users to change their passwords and to be aware of phone calls made from the "650" area code.Google's response team acted swiftly to terminate unauthorized access, revoke credentials, and notify affected clients. The company has also updated its policies around connected app authorizations and is working closely with law enforcement

Subsequently, Salesforce has decommissioned all tokens linked to the breach and alerted their customers. Zscaler has also verified that the impact from the breach will be widespread, affecting many businesses outside of the ones mentioned above.This experience is a stark lesson for many in terms of our greatest weakness in the technology space, which is human error. For this reason, industry leaders including Salesforce and Zscaler are heavily focused on creating a secure digital environment.

How can we protect ourselves from vishing?

As everyday users and customers of large tech companies, there's little we can do in the face of organised cyber crime groups. Keeping yourself personally safe from scams means staying constantly vigilant but we as individuals and companies can also be proactive about reducing the risk of being targeted by vishing tactic.

To avoid similar situations in the future you should be implementing stricter verification procedures to tie new applications to an organization and authorize OAuth tokens with SaaS providers. This also means multi-factor authentication must be mandatory across the board, and constant audits must be performed to verify those connections. Organizations can build awareness of these tactics and must conduct realistic/simulation-style training to build employee resilience against vishing and phishing attacks. They can also use additional verification methods, such as on-camera checks, Geo-verification, or by asking questions that cannot easily be answered with information found online.

This breach has demonstrated that the weakest link in cybersecurity is not the design of a software program, but rather the inherent trust that exists between individual people and the companies that employ those individuals. Implementing effective awareness and robust preventive security measures are the only ways for companies to maintain protection against rapidly evolving threats such as ShinyHunters.

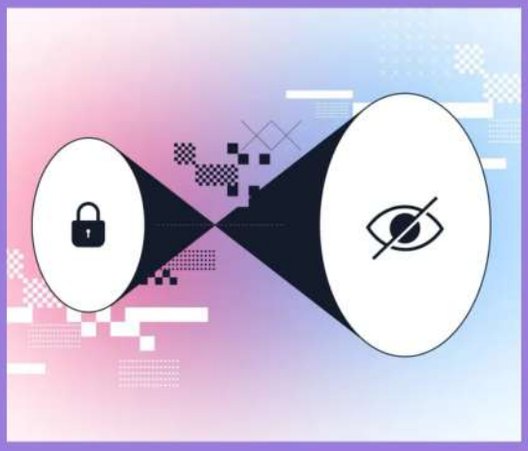
ETHICS IN AI AND CYBERSECURITY

The landscape of AI integration in various domains changes rapidly with an increase in compute resources and methodologies. Cyber security is no exception as the ethical considerations that bothered security researchers during the advent of the AI hype were not the same as the concerns during the peaks through 2024-2025. This article aims to use the structure of several essays from the time period to provide a comparative analysis of how concerns, approaches, and limitations have changed during the two years.

PRIVACY VS SECURITY

One of the biggest concerns in developing a security framework is the trade-off between privacy and security that a program can offer. They are often seen as the two ends on a sliding scale, where increasing the importance of one, risks the other. However, such an approach is based on that presumption. Practically, while there are certain instances where compromising user privacy can offer insights that improve the security of a service, it is generally the case that they are mutually exclusive, if not directly proportional.

For example: Zero-log policies can improve privacy and remove risks of data breaches.



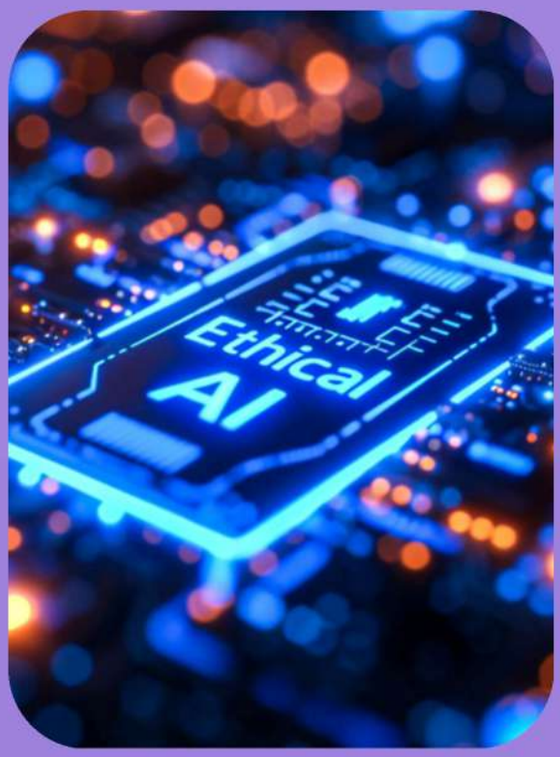
BIAS

Amidst the hype of generative AI, concerns rose about the bias of classification models to mislabel sections of society underrepresented in the training data. The focus of data sciences and training data collection for SOTA (state of the art) models have matured significantly since the early models and now focuses on accounting for over-representation as well as under-representation of a sub-section.

Research into this specific issue has existed since long before the Gen-AI hype and each offers novel solutions for the issue, ranging from synthesis of data, to equalization and normalization. When discussing the specifics of cyber security, the use of pragmatic models that do not account for diversity can often log natural behavioral differences as threats.

ACCOUNTABILITY

One of the questions that has bothered security executives and developers alike is, "Who takes the fall when AI makes a mistake?". Whether it should be people who created the training data, the people who purchased or stole it to train ML models, the SaaS company hosting the model behind abstractions, the security personnel who decided to implement the model, the developer using the model, or the attackers exploiting its vulnerabilities. The field is unregulated and abstracted enough for teams to hold any scapegoat responsible for any mishap. The lack of real legal regulations and the inefficacy of copyright laws worsens the situation.



JOB DISPLACEMENT

As companies awaken to the limitations and technical debt that follows replacing human labor with AI tools and unskilled interns, the demand for skilled cyber security specialists increases steadily, accelerated further by the threat of use of AI in hyper targeted cyber attacks.

THE INDIAN CONTEXT

Over the last couple of years, India has seen a massive leap in growth and development of its cybersecurity sector even though cases of ransomware grew with each passing year. From sending out a simple text message to initiating a monetary transaction to a huge financial institution holding customer data, or the government keeping masses of data on all Indians, the sole dependency for all digital systems relies upon one entity, that is, security.

Three major cases recently came under public scrutiny in India- The Aadhaar Data Breach Controversy (2018), The BigBasket Data Breach (2020) and The AIIMS Delhi Cyberattack (2022).

The Aadhaar Controversy in 2018 put in light protection of Identity data within the nation. The largest biometric identification system of India was exposed to unauthorized access easily attainable by just clicking and buying over the illegal internet marketplaces put in alert for misuse of data, even though later authorities denied the scale, it had instilled a strong fear among citizens, and had left a very heavy scar on the country's digital footprint of implementing sophisticated encryption, data governance protocols and a strong access control system to our central databases.

Cyber attack causes chaos, delay in services at AIIMS, probe launched

ASHISH SRIVASTAVA @ New Delhi

CHAOS ensued at the Centre-run All India Institute of Medical Sciences on Wednesday after the apex institute witnessed a cyber attack on its main and back-up server, which adversely affected the patient care services in the hospital, sources said.

After the attack, both the server faced shutdown. A team of cyber experts from the National Informatics Centre cut off the link of the second back-up server to prevent further damage, sources added. However, the cyber attack has corrupted all the files stored on main and back-up servers of the hospital. Tech experts are trying to recover the lost data, sources said.

The incident led to disruption in a range of hospital services, including appointments and registration at the out-patient department, billing at the in-patient department, laboratory report generation, and smart lab, among others.

However, the hospital did not wholly confirm the cyber hacking and only shared the possibility of a ransomware attack on its e-hospital feature which was recently integrated to facilitate patient care services digitally. "The National Informatics Centre team working at AIIMS has informed that this may be ransomware attack which is being reported to and will be investigated by appropriate law enforcement authorities," the hospital said.

Sources also said he demanded a huge amount by email with a warning that the extent of the cyber attack could also extend to other services. Meanwhile, a probe has been launched, with AIIMS reporting the incident to police.

The outage caused tremendous inconvenience to patients, as several services which were recently integrated into the e-hospital manual to facilitate digital delivery of facilities in the hospital, had to be done manually, leading to hassle and delays. "With the server being down, the OPD and sample collection were handled manually but the sample system for those who do not have a Unique Health Identification was affected. The patients were not able to register themselves or make an appointment digitally or on site for a very long time," a source said. The cyber attack comes close on the heels of AIIMS announcing complete digitisation of all hospital services by April 2023.

With the server being down, the OPD and sample collection were handled manually but the sample system for those who do not have a Unique Health identification was affected

Official source

In another event of similar circumstances, the BigBasket data breach in 2020 put a lot of concerns among users regarding security of data kept in private sectors as cyber attackers gained access to large quantity of consumer' data (emails, phone numbers, passwords etc.). Data also suggested that this hacked information was sold over dark web markets and once again brought to spotlight on necessity of maintaining an aggressive stance against any threat through constant penetration testing and vulnerability assessment.

One of the premium medical institutes of India, All India Institute of Medical Sciences, New Delhi holds several thousands of records on patient's care, hospital management and researches; the cyberattack had imposed huge risk on patients' privacy and more significantly on health and safety of its citizens because the attack disrupted a huge part of its services, the suspected group LockBit ransomware group demanded payment of Rs 200 crore in crypto currency and the AIIMS server was completely out of service for a span of six continuous days.

The Indian government now must look forward that cybersecurity is more of a matter of national resilience and integrity rather than merely a privacy issue. Laws related to data protection must be enforced with sheer accountancy. The government must consider in increasing its budget for acquisition of better security systems and keep the nation's infrastructure safe.

Author : Tejaswini Nayyar

SECURITY IN EMERGING TECHNOLOGIES

This can be seen clearly as AI, quantum computing, and the Internet of Things(IOT) become more integrated into our global infrastructure. This means that we have a much larger attack surface, and it is growing exponentially. The technologists are largely responsible for keeping these emerging technologies secure, often before defences are even thought of. With AI, for example, there is a growing concern with adversarial machine learning, which attempts to manipulate the training data used by the AI system. This changes the threat model so that the logic used by the AI appears to be compromised, not just its data.

Quantum computing, or as it has come to be referred to, the coming "cryptographic apocalypse," is something that should be examined a bit more closely as the tech world continues its path to cyber-preparedness. For Example like in Encryption there are many different standards that are used, and they are dependent upon mathematical problems that can be solved by a supercomputer in a blink of an eye. Instead of waiting for an apocalypse, experts should be using Post-Quantum Cryptography. However, this can only be accomplished if we are able to change these standards without changing their fundamental configuration.

In the world of IoT, the actual obstacle isn't the number of connections, but the sheer number of low-power devices that can't deliver the horsepower for robust encryption. Wearable medical equipment, industrial sensors, and other lightweight technologies have, in the past, been the key to wide-ranging botnet attacks. But to create a cyber-ready world, we need to adopt a concept of Security-by-Design, where every autonomous algorithm is tested before it's put into production. It's time to move away from the old "patch later" mentality of the early days of software and make security a fundamental, non-negotiable requirement.

As we bring data processing closer with the advent of 5G technology and edge computing, the opportunities for security are arising in new ways. Experts need to consider the scenario of processing data at the origin, which is far from the reach of the data centre for the purpose of safeguarding. This brings us to the hardware-centric concept of security, which involves the concept of trusting the hardware that runs the software. In short, it provides an opportunity for trusting the system even if the software is breached.

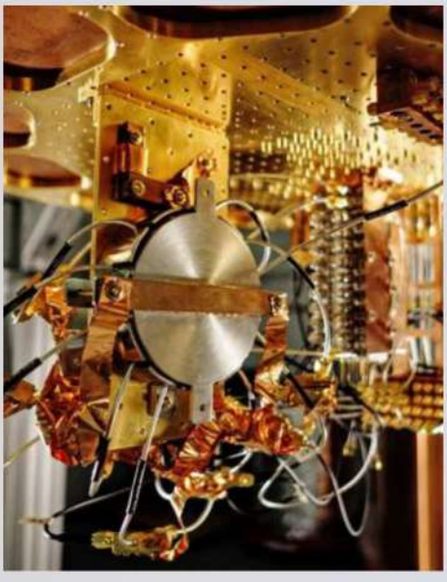
But the goal of the technocrat of today is not only for the system to be secure, but also for it to be resilient. The route to such a goal of resilience is one where the system can fail, but can also heal itself.As autonomous technology becomes increasingly part of the mix, the technocrat's place changes, not only from one of direct management, but also one of strategic management, while keeping humans in the loop as a true safeguard against bias and exploitation.

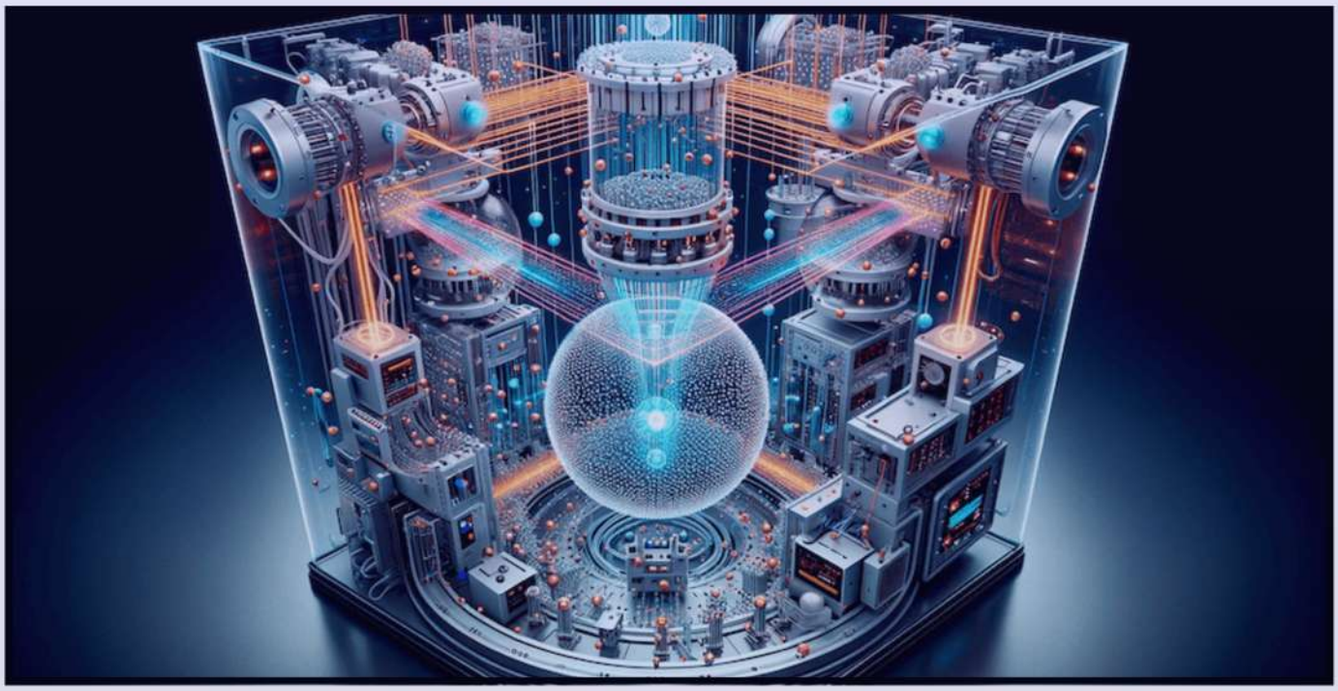
WHAT A QUANTUM FUTURE MEANS FOR CYBER SECURITY

Modern cybersecurity is greatly dependent on cryptographic schemes such as the RSA and elliptic-curve encryption algorithms. The latter is based on the difficulty of performing certain complex mathematical calculations using classical computers. However, these problems can be solved efficiently on a sufficiently powerful quantum computer, rendering such a device capable of decrypting data that is currently considered secure. One of the main security concerns in this scenario is the "harvest now, decrypt later" concept where data is collected now and will be encrypted only later when quantum computers are available.

As industries, business networks and cloud computing services are heavily reliant on digital networks, security of data against the threat from emerging technological capabilities has become a paramount concern for everyone across the world. Consequently, a number of cybersecurity professionals are investigating new ways of coping with what many experts call the "quantum era" of computing. A few such approaches toward developing quantum resistant cybersecurity systems are discussed below:

Post-quantum cryptography (PQC) :
This concept suggests the design of cryptographic algorithms that would be secure against quantum computer attacks. Unlike the current cryptography systems that depend on the intractability of certain mathematical problems on a classical computer, PQC would rely on math problems considered difficult on both quantum and classical systems. It is considered to be a crucial component to secure digital infrastructures of the future.





Various organizations and governments are developing various standards for such cryptographic algorithms so that they are readily available to the users across the internet to use as an replacement of current encryption systems.

Quantum key distribution (QKD) :
Instead of depending on complex mathematical algorithms, this method relies on the laws of physics for encryption. Encryption keys are transmitted to respective parties through particles like photons. Any interruption during the transfer would immediately collapse quantum properties of photons, alerting both sender and receiver of the fact that the message is being intercepted. Although this system offers great security, its implementation requires special equipment and infrastructure that would not be feasible in the current environment.

AI-driven security systems :
The AtI based security systems could effectively scan huge amounts of data and identify potential threats that are invisible on classical security systems. Certain cyber-security researchers are hoping that by combining AI with quantum computing principles, we can evolve highly effective threat identification and response capabilities that would not be possible otherwise.

There are a few hurdles for adoption of these quantum resistant techniques:

- Huge existing systems that would need extensive upgrades to implement new algorithms and software.
- The overall cost to integrate the new technologies would be too high.
- Difficulty in estimating when quantum computers would be capable to provide such a threat, therefore hindering long-term planning for these massive upgrades.

However, with the continuous growth of quantum computing technology, cybersecurity systems must evolve. Experts generally agree that the adoption process should commence much before qantum computers actually start making an impact.

Cyber Security and Innovation

Cyber security is a vital element of all modern technology. In this era of internet dependency, threats have amplified, increasing both the frequency and the sophistication of cyber attacks. There is consequently an unprecedented need to continually innovate on security technologies. The origins of this innovation can come from tech companies, universities and research institutions, through industry publications or competitive events like hackathons.

Company & Research Institution Innovations :

Microsoft, Palo Alto Networks and CrowdStrike are some of the most innovative in AI-driven threat detection, next generation firewalls, cloud security applications and zero-trust security networks. A relevant example is Microsoft's Defender for Endpoint which uses machine learning to detect ransomware and malware threats in real time. This form of analysis along with behavioral detection are areas in which Microsoft continue to innovate. Palo Alto Networks has designed cyber security mesh architectures which pull multiple security tools together within distributed environments, offering greater agility in solutions.

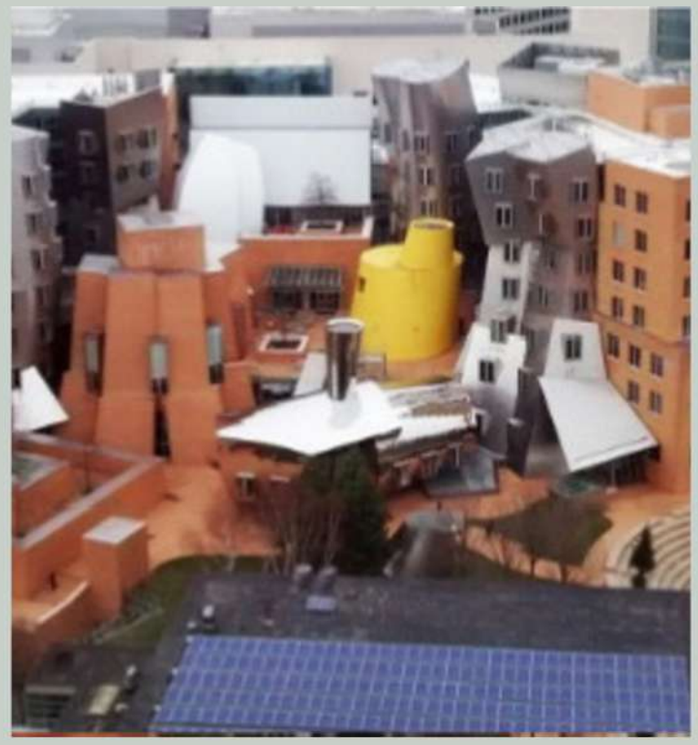
Universities including MIT, Stanford and IIIT Hyderabad conduct research in exciting new areas including quantum-resistant encryption, blockchain security and AI driven threat detection. The computer science and AI laboratory at MIT (CSAIL) have prototyped software designed to prevent internet-connected devices from falling victim to novel malware. Researchers at Stanford University have been examining the applicability of machine learning to network threat analysis; results from their experiments suggest they can already detect computer intrusions before a human user has a chance of even doing so.

Student Innovations :

The contribution to cybersecurity innovation by students through their participation in universities, competitions and hackathons can also be significant, developing both practical applications and futuristic models of how to secure digital assets.

AI-Powered Threat Detection Tools :

One particular area in which students have made some remarkable contributions is the development of AI for threat detection. There has been a widespread development of machine learning models designed to detect malicious network behavior and phishing attempts by students eager to identify the underlying patterns that define an attack. Platforms capable of analyzing emails and flagging scams were featured and developed in national hackathons.
Deepfake and Digital Content Verification



Deepfake and Digital Content Verification :

The development of technology for deepfake and digital content verification is another area where students are active. With artificial intelligence making it easy to generate authentic-see ming images and videos, it is vital that we are equipped with tools to discern legitimate content from falsified versions. Some technologies go as far as detecting minute flaws in expressions and voice patterns, indicating manipulation. Others are capable of scanning for digital signatures in the media.

Blockchain-Based Security Applications :

In an interesting niche, students have also explored the creation of security applications using blockchain. From data security and digital authentication platforms that employ the immutability and distributed ledger of the blockchain, to vote security applications and tools that authenticate documents and verify their origins, the potential of the technology for security seems vast and is being widely researched.

Many of these student applications contribute to the broader cybersecurity domain, ultimately influencing the technology of tomorrow, and further refined by startups and tech companies to provide the solutions needed for the digital world of the future, giving everyone who interacts with it a better, more secure experience. It is these student innovations, in conjunction with advances in large corporations and academic institutions, that will build the secure systems required to protect the internet of tomorrow.

AI IMPACT SUMMIT
भारत 2026 INDIA

सर्वजन हिताय | सर्वजन सुखाय

WELFARE FOR ALL | HAPPINESS OF ALL

INDIA-AI IMPACT SUMMIT 2026

The India–AI Impact Summit 2026, was suffice to say the biggest AI tech gathering in the world till date, it was more than your everyday technology conference, it was a global gathering which marked a defining global inflection point.

THE SEVEN CHAKRAS

The AI summit was structured around the following seven working thematic groups:

1. Human Capital
2. Inclusion for Social Empowerment
3. Safe and Trusted AI
4. Resilience, Innovation and Efficiency
5. Democratizing AI Resources
6. Science
7. AI for Economic Growth and Social Good

The Summit focused on three foundational pillars or "sutras":

People – AI must serve, the **people**.
Planet – AI must sustain, the **environment**.
Progress – AI must advance, the **economy**.

The India-AI Impact Summit hosted over 6 Lakh attendees, and delegates from over 100 countries which included 500+ global tech leaders and CEO's such as Google's Sundar Pichai, OpenAI's Sam Altman, Anthropic's CEO Dario Amodei, Qualcomm's President & CEO Christiano Amano, Vice Chairman of Microsoft Brad Smith, and many other distinguished participants from across the globe. Their presence further bridged the gap between AI oriented commerce and research, hinting at future collaborations and growing dependencies between industries.

India has the second largest AI workforce in the world, and provides over 20 percent of the world's data and over 700 million internet users. AI companies are already spending billions on developing infrastructure and workforce training in India.
Including examples such as-

- Microsoft invested $17.5 billion over 4 years to expand AI infrastructure in India.
- Google announced a new America-India Connect which introduces a new fibre optic route between the US and India to advance global AI access.
- NVIDIA plans to build India's largest gigawatt-scale AI factory.
- Adani announced to invest $100 billion for renewable powered AI data centres.
- Google plans to train more than 20 million public servants across 800+ districts through partnerships with Karmayogi Bharat.
- OpenAI has tie ups with IIT Ahmedabad AIIMS to educate more than 5 Lakh students.

Another initiative among others were :

'AI for All and AI by HER.'

The former strives to identify solutions that use AI to enable large-scale impact and the latter is a global innovation challenge that invites women technologists to present AI solutions that address real world concerns. These projects are carried out by Startup India under the Department of Promotion of Industry and Internal Trade(DPIIT) and the Women Entrepreneurship Platform of NITI Aayog respectively.

Author : Pragya [BCA, 3rd Year, Shift-1]

TECHNOWHIZ

GLIMPSES FROM THE PAST

EDITORIAL TEAM

CONTENT LEAD
Himanshi Tomer
BCA, 3rd Year

DESIGN LEAD
Muskan Kashyap
BCA, 3rd Year

CONTENT TEAM

Druhi Mehra
3rd Year, Shift-1

Tejaswini Nayyar
3rd Year, Shift-1

Anushree
2nd Year, Shift-1

Aditya Pratap Singh
2nd Year, Shift-2

Anshita
2nd Year, Shift-2

DESIGN TEAM

Saanvi Narula
3rd Year, Shift-1

Pragya
3rd Year, Shift-1

Chirag
2nd Year, Shift-1

About JIMS

Jagan Institute of Management Studies (JIMS) carries a rich legacy spanning over three decades in delivering professional education at both undergraduate and postgraduate levels in the fields of Management and Information Technology. With an unwavering commitment to developing competent industry professionals, the Institute is recognized as one of the leading business schools in the country. Our PGDM programs are approved by the All India Council for Technical Education (AICTE) and hold accreditation from the National Board of Accreditation (NBA) for their quality academic standards. The programs are also accorded equivalence to the MBA degree by the Association of Indian Universities (AIU). Our GGSIP University affiliated programs are MCA, BBA, BCA and BA (H) (Eco.). The MCA programme is also accredited by the National Board of Accreditation. The institute also runs AICTE approved Fellow Program in Management has been accorded equivalence to Ph.D degree by the AIU. Further affirming our commitment to academic excellence, JIMS has been awarded them NAAC A++ grade and secured SAQS accreditation
from AMDISA, placing it among the most respected institutions in management education. JIMS Rohini, Delhi proudly attained Graded Autonomy Category II recognition from AICTE. JIMS Rohini, Delhi also continues to remain in the list of elite B schools of India (Top 100) for 10 years in a row since the inception of ranking in 2016. Apart from providing gainful and decent placements to its students, JIMS also encourages the spirit of entrepreneurship. The Institute proves to be an ideal place for those wishing to engage in academic pursuits and to seek intellectual fulfilment. The institute also runs AICTE approved Fellow Program in Management which is equivalent to Ph.D degree.

Jagan Institute of Management Studies
3, Institutional Area, Sector-5, Rohini (Near Rithala Metro Station), Delhi-110085
+91 45184000/01/02 | +91 45184032 | +91 7827938610
contact@jimsindia.org
www.jimsindia.org