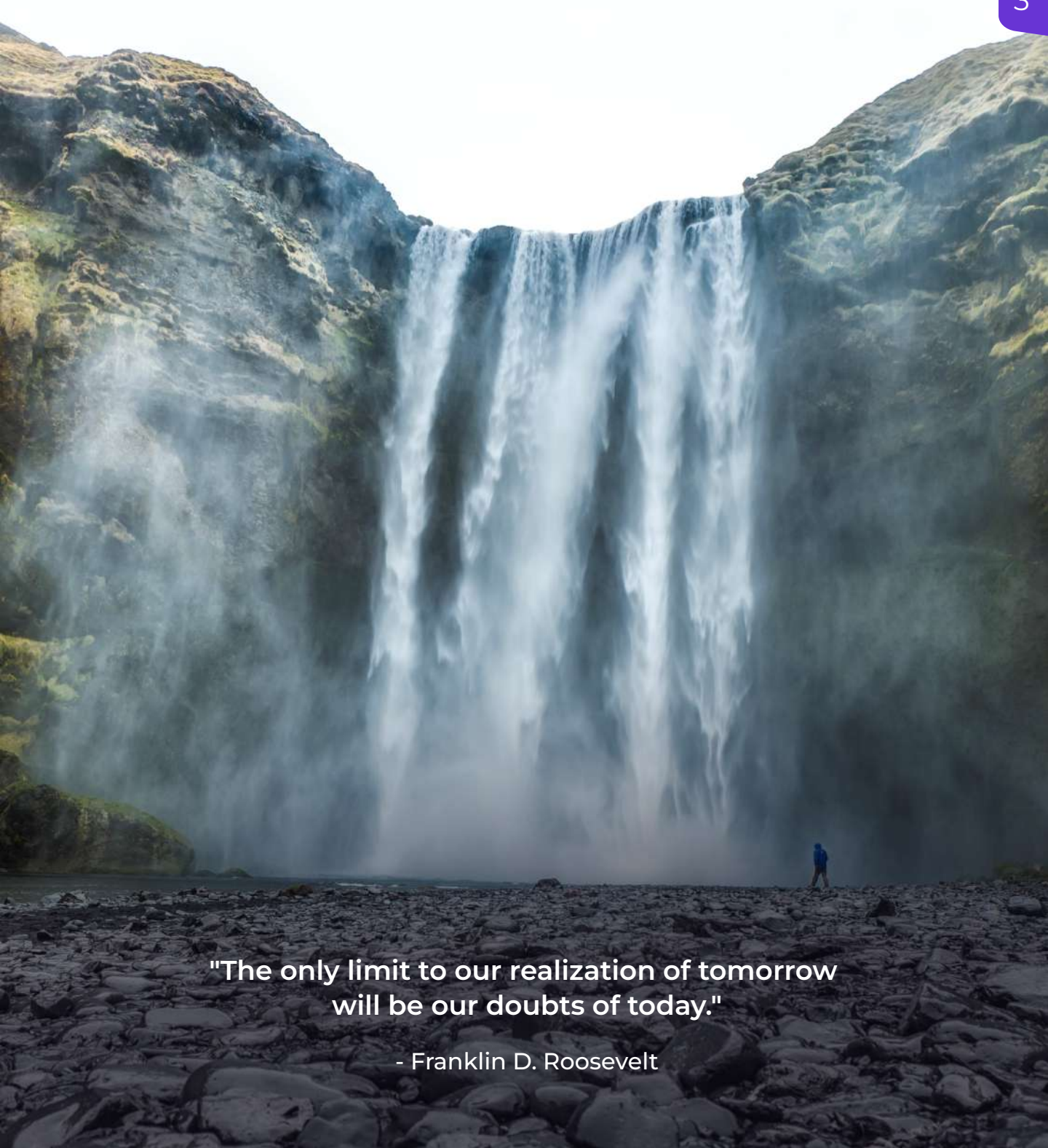
enGAge

Sep 23



"The only limit to our realization of tomorrow will be our doubts of today."

- Franklin D. Roosevelt

Table Of Content

Editor's Note

Soumika Das

In recent times, there has been a noticeable push to make artificial intelligence more accessible. Just this July, Meta took a significant step by releasing Llama 2, a potent AI model, for anyone to freely download, modify, and reuse. This move has gained immense popularity among various groups, including companies, researchers, and enthusiasts, as they harness Llama 2's capabilities akin to ChatGPT.

However, the concept of making AI "open" is not as straightforward as it seems. Llama 2 is free to download, modify, and deploy, but it is not covered by a conventional open source license. Meta's license prohibits using Llama 2 to train other language models, and it requires a special license if a developer deploys it in an app or service with more than 700 million daily users. This raises the question of what it really means for an AI model to be "open." Some researchers, from Carnegie Mellon University, the AI Now Institute, and the Signal Foundation, argue that the term is often used in a misleading way, and that many models that are branded "open" are actually quite restrictive. Their research has uncovered that the usage of terms like "open" and "open source" in the context of AI can be "confusing and diverse". Often, these terms hold more aspirational or marketing value than technical accuracy, blending notions from both open source software and open science.

A research paper states that despite a few genuinely open AI systems that offer extensive transparency, reusability, and flexibility, the resources required to build and deploy large-scale AI systems remain largely inaccessible, residing with corporations that hold substantial resources.

The challenges of genuine openness in AI are multifaceted. The computational power needed for training a large model is often expensive, typically requiring tens or hundreds of millions of dollars for a single training run. The human expertise required to improve these models is usually concentrated within well-funded companies. Also, the data necessary to train advanced models is often kept a secret.

"Open" AI can provide transparency, reusability, and extensibility that can enable third parties to deploy and build on top of powerful off-the-shelf AI models. However, they also caution that even the most open of "open" AI systems do not, on their own, ensure democratic access to or meaningful competition in AI. In essence, while efforts to make AI more open are commendable, a nuanced perspective is necessary to navigate the intricate landscape of AI accessibility.

We have a lineup of insightful articles in this edition.

Rajeswari S has written, **Healthcare Revenue Cycle Management Part 2.**
Bhavani Damodaran has written, **Cyber Resilience in the Age of Ransomware: Strategies for Organizations.**
Team UNBOX has written, **Design Sprints Part 2 – Application of Design Sprints.**

Happy Reading!

What's New in Tech

Multimodal AI Model for speech and text translations

Meta has introduced 'SeamlessM4T,' an advanced AI translation model that performs speech-to-text, speech-to-speech, text-to-speech, and text-to-text translations in nearly 100 languages. The model also marks a significant milestone in the field of AI by releasing the metadata of SeamlessAlign, an extensive multimodal translation dataset encompassing 270,000 hours of speech and text alignments.

Sharing chemical knowledge between human and machine

Researchers have developed a platform that uses artificial neural networks to translate chemical structural formulae into machine-readable form. Using this platform, they have established a tool that can automatically input such data from scientific publications into databases. Previously, this task required manual intervention and was a labor-intensive process.

Self-supervised AI learns physics to reconstruct microscopic images from holograms

Researchers at the UCLA Samueli School of Engineering have unveiled an AI-based model for computational imaging and microscopy without training with experimental objects or real data. The self-supervised AI model nicknamed GedankenNet learns from physics laws and thought experiments. Informed only by the laws of physics that universally govern the propagation of electromagnetic waves in space, the researchers taught their AI model to reconstruct microscopic images using only random artificial holograms, without relying on any real-world experiments, actual sample resemblances or real data.

Thermal imaging innovation allows AI to see through darkness

Researchers at Purdue University are advancing the world of robotics and autonomy with their patent-pending method that improves on traditional machine vision and perception. They have developed HADAR, or heat-assisted detection and ranging. It is expected that one in 10 vehicles will be automated and that there will be 20 million robot helpers that serve people by 2030.

Healthcare Revenue Cycle Management

Part 2

In the previous article, we explored what is Healthcare RCM, who are its stakeholders and their roles, the types of payers - Government and Private, and the various activities performed by Front Office and Claims Office in the RCM process.
You may read it here:
https://www.gavstech.com/healthcare-revenue-cycle-management/

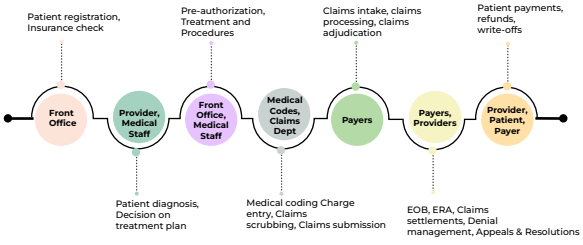
In this article, I will take you through the duties of the Back Office, functional flow of RCM from start to finish, importance of RCM in healthcare and the role of technology in RCM industry.

To reiterate the concept, Revenue cycle management (RCM) is the process followed by healthcare systems all over the world to maintain and track their revenue for the services rendered to patients. It is a major stream of work in the healthcare ecosystem which involves clinical, administrative, and financial functions. These functions enable healthcare providers to capture, manage and collect their patient service revenue.

Back Office

In the whole of the above process, there is a lot of communication and coordination that happens between the patient-provider-payer as back-end activity which includes claims status check, denial analysis, appeals, amount to be settled or refunded to patient, write-offs, and so on.

To visualize the flow:



Why is RCM important?

An efficient RCM system enhances a hospital's revenue stream. It considerably reduces the time between care services given and payment received. It connects the commercial and clinical aspects of healthcare.

CMS views denials as a crucial non-performance factor on the hospital side. Hence, hospitals must keep their number of denied claims to the utmost minimum. RCM process help hospitals in achieving this.

> Denials rose to 11% of all claims last year, up nearly 8% from 2021, according to a recent study. That 11% rate translates into 110,000 unpaid claims for an average-sized health system, according to the report. Cost of denials saw 67% increase in 2022.
>
> Source : HealthLeaders

RCM process help providers to reduce errors in claims processing, improve patient experience, speed up claims submission and bring down reimbursement cycle time. RCM process bridges the gap between service providers and insurance firms, which eventually improves the RCM turnaround.

Role of technology in RCM Industry

The RCM industry is anticipated to experience substantial changes and growth in the coming years. Technological progress, including artificial intelligence and machine learning, will play a crucial role in automating and streamlining RCM procedures, resulting in decreased administrative expenses and faster revenue cycles. The following technologies will play a crucial role in RCM:

- Blockchain for handling transaction surge, revenue velocity and payment accuracy
- RPA - Robotic Process Automation for bringing in digital workforce to improve efficiency and reducing errors
- Big data and analytics to stop revenue leakage, improving date integration, processing, and management
- AI/ML to alert denial risk, medical coding error detection, claims admin, denial recovery, etc.

Major players in the global RCM market

Some major players in the global RCM market include R1 RCM, Oracle, and Optum. Other prominent players include McKesson Corporation, GE Healthcare, Cognizant, 3M, and Athenahealth.

RCM is a critical process for healthcare organizations to ensure that they are properly reimbursed for the services they provide. Technology is playing an increasingly important role in RCM, with solutions such as blockchain, robotic process automation, and big data analytics helping to automate and streamline RCM processes. Overall, the future of the RCM industry holds immense potential for innovation, efficiency, and improved financial outcomes for healthcare organizations.

About the Author

Rajeswari is part of the Solutions and Strategy team at GS Lab | GAVS. She has been involved in technical and creative content development for the past 15 years. She is passionate about learning new technologies, gardening, music and writing. She spends her free time watching movies or going for a highway drive.

Rajeswari S

Cyber Resilience in the Age of Ransomware

Strategies for Organizations

With the ever-evolving IT Infrastructure and rapidly evolving threat landscape no organization today can truly say we are immune or safe from cyber-attacks. There are several factors that contribute to the rise in ransomware attacks. One key factor to note is the sophistication of the ransomware gangs. These days the ransomware gangs are equipped with the latest in technology and sophisticated techniques to infiltrate networks and encrypt data. Another factor is the growing availability of ransomware-as-a-service (RaaS) platforms. This makes it easy for even inexperienced hackers to launch attack on organizations.

There are several cyber-attacks taking place around us. And more specifically, the number of ransomware attacks has increased significantly each year and in the year 2023, there are about 10,000 attacks reported in the first quarter alone. This is a significant increase from 2022 for the same period.

Cyber resiliency pertains to an organization's capacity to endure, adjust to, and bounce back from cyber-attacks or any other forms of malicious activities. It aims to limit the adverse effects on an organization's operations, data, and overall functionality. Cyber resiliency encompasses a comprehensive set of tactics, procedures, technologies, and methodologies that are implemented to sustain an organization's optimal functioning despite prevailing cyber threats.

Cyber resilience presents various advantages to an organization, which include :

1. Minimized Financial Losses: Through the implementation of cyber resilience measures, an organization can reduce the financial impact caused by cyber-attacks, such as asset theft, revenue loss, and repair expenses.

2. Compliance with Legal and Regulatory Requirements: Cyber resilience measures aid organizations in meeting legal and regulatory mandates concerning data protection, security, and privacy.

3. Enhanced Security Culture and Internal Processes: By prioritizing cyber resilience, an organization can cultivate a robust security culture and establish efficient internal processes to address cyber risks effectively.

4. Safeguarding of Brand and Reputation: Cyber-attacks can tarnish an organization's reputation and brand. However, by adopting cyber resilience, organizations are better prepared to prevent cyber-attacks, respond promptly and efficiently to incidents, and maintain the trust of customers and stakeholders.

While we understand the benefits of a cyber resilience program it is imminent to note that the IT Governance framework provides guidelines for implementing effective cyber resilience within an organization. It consists of four key elements:

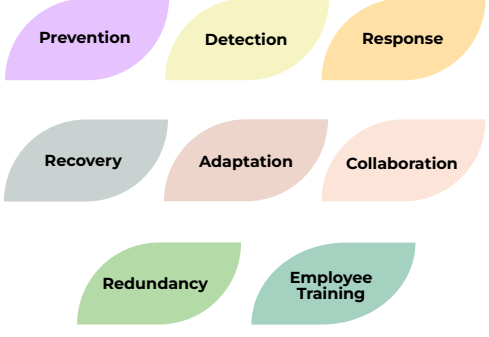
1. **Manage and Protect**
   - Focus on managing defences and protecting the organization from cyber threats.
   - Includes implementing an information security program, policies, identity and access control, training and awareness, as well as physical and logical security measures.

2. **Identify and Detect**
   - Monitor the organization's information and information systems for anomalies.
   - Continuously observe and log security measures, conduct vulnerability and penetration testing, and actively detect potential incidents.

3. **Respond and Recover**
   - Quickly and effectively manage incidents to minimize damage and restore functionality.
   - Have well-documented incident response and business continuity plans in place.

4. **Govern and Assure**
   - Involve the board and senior managers in overseeing and validating cyber resilience at the highest level of the organization.
   - Implement a robust risk management program, conduct external audits or validations, and perform internal audits.

Also, further in-depth classification of the areas above is listed below.



- **Prevention:** Preventive measures aim at reducing the likelihood of an attack taking place. It comprises of implementing robust cybersecurity measures to prevent cyberattacks, including firewalls, intrusion detection systems, access controls, and regular security audits.

- **Detection:** Employing advanced monitoring and detection tools to identify unusual or suspicious activities within the organization's network or systems. This helps in detecting cyber threats as early as possible.

- **Response:** Developing well-defined incident response plans that outline the steps to take when a cyber incident occurs. This involves isolating affected systems, mitigating the impact, and taking appropriate measures to prevent the incident from spreading further.

- **Recovery:** Establishing procedures and protocols for recovering from cyber incidents and restoring normal operations. This may involve data recovery, system restoration, and ensuring the organization's critical functions can resume.

- **Adaptation:** Continuously evaluating and improving cybersecurity practices based on the lessons learned from previous incidents. This includes updating policies, procedures, and technologies to address new and evolving threats.

- **Redundancy:** Implementing redundant systems and data backups to ensure that critical operations can continue even if primary systems are compromised.

- **Employee Training:** Providing ongoing cybersecurity training to employees to increase awareness of potential threats and best practices for mitigating them.

- **Collaboration:** Building partnerships with external organizations, such as law enforcement agencies, cybersecurity experts, and other industry stakeholders, to share threat intelligence and coordinate responses to cyber incidents.

Zero Trust Architecture

The concept of Zero Trust Architecture (ZTA) has acquired meaningful traction in recent age. This approach operates on the assumption that no user or system should be innately trustworthy, regardless of their location inside or outside the network. ZTA focuses on validating identities and continually listening to network traffic and user attitude to discover deviations. By adopting this approach, organizations have better control over their network and reduce the attack surface.

Extended Detection and Response (XDR)

XDR goes further than Endpoint Detection and Response (EDR) and includes the listening of various endpoints and security tiers across an organization's IT foundation. This whole approach allows for better threat discovery by correlating data from multiple sources and providing an extensive view of potential security incidents. XDR solutions allow institutions to respond promptly to emerging risks and prevent them from spreading across other systems.

Cloud Security Resilience

The increased acceptance of cloud services has driven an increasing importance of cloud security resilience. Organizations are establishing tools and strategies to secure their cloud environments effectively. This contains executing correspondence and access administration controls, encrypting sensitive data, and monitoring for unauthorized access or configuration changes. As more critical operations move to the cloud, guaranteeing its protection has become a principal concern.

AI and Machine Learning in Cyber Resilience

Artificial Intelligence (AI) and Machine Learning (ML) are performing an important role in helping cyber resilience. These technologies can resolve boundless amounts of data in real-time, recognizing patterns and irregularities that go unnoticed by usual security measures. AI-stimulation systems reinforce warning discovery, automate incident reaction, and advance the overall effectiveness of cybersecurity operations.

Ransomware Preparedness and Recovery

The surge in ransomware attacks has necessitated efforts to strengthening ransomware preparedness and recovery. This involves frequently backing up critical data, evolving occurrence response plans particularly tailor-made to ransomware occurrence, and conducting cybersecurity training for staff members. Proactive measures can considerably reduce the impact of ransomware attacks and help reduce the reaction time to cyber-attacks.

Supply Chain Cybersecurity

Organizations' cybersecurity is only as strong as the weakest link in their supply chain. As a result, there is a growing need on assessing and ensuring the cybersecurity posture of third-party vendors and partners. Rigorous evaluations, permissible contracts, and constant monitoring are suitable standard practices to lighten supply chain-accompanying high-tech risks.

In an era defined by digital revolution, cyber resilience has surpassed the world of IT and is critical to all businesses. Cyber resiliency recognizes that despite best efforts in preventing cyberattacks, determined attackers may still find ways to breach defences. Therefore, the focus is on minimizing the impact of such breaches and ensuring that the organization can recover quickly and effectively. In this article, we cover the evolving types of cyber threats, and the innovative approaches organizations are adopting to improve their strength to endure and bounce back from potential attacks. As the threat landscape develops, staying informed about these trends will be essential for organizations planning to build a powerful and adaptable cybersecurity framework. Cyber resilience is a holistic approach that goes beyond traditional cybersecurity measures to encompass broader organizational preparedness and adaptability.

About
the Author

Bhavani is a Technical Manager, Information Security at GS Lab | GAVS. She has held numerous positions of responsibility in areas of Information Security such as risk management, IT controls, audits and compliance. Her expertise involves in handling IT risks, security control framework designing and assessing digital tools. She is an avid traveler and is passionate about driving.

Bhavani Damodaran

Design Sprints

Part 2 – Application of Design Sprints

Design sprints are a collaborative process that helps teams quickly brainstorm and iterate on ideas. The time-bound setup allows team members to be productive. In the first part of this design sprint series, we discovered the concept of design sprints and the steps involved. This blog focuses on productivity and the application of design sprints.

Design Sprints and Productivity

Design sprints bring people from different departments and leverage prototyping and usability testing to arrive at solutions. Most organizations adopt design sprints where the goal is already defined. For instance, design sprints are a better-suited process when a user experiences problems such as high bounce rates or low sign-ups. In these situations, the team can break down the user journey and identify the problem area to arrive at a better solution.

However, for design sprints to succeed, it is essential to manage expectations. The idea of design sprints is not to arrive at the perfect solution but to brainstorm new concepts quickly and gain feedback from the team relatively faster. By setting the expectation, members of the design sprint process can work towards bringing as many ideas as possible instead of worrying about their viability, thus improving the team's productivity.

The following points must be considered for a design sprint to be truly productive:

- The goal of the sprint – It can be anything from increasing the number of sign-ups to reducing the steps to account creation.
- Problem statement – Unless a defined problem exists, it isn't easy to succeed with the design sprint process. A problem statement can be anything from a high drop-off rate or a website loading time issue.
- Defined target group – This helps understand the user perspective and develop customized solutions to suit their needs.
- Pain points or constraints – There needs to be an understanding of the current difficulties creating the problems in the first place
- Time to launch – Time is of the essence and hence the team needs to align their process to ensure adherence to timelines set for launch.
- Team members – It is important to have a good mix of members with varied skillsets and from diverse roles in the organization so that the ideas are holistic.

Benefits of Design Sprints

Design sprints, when done right, can benefit a business in many ways.

- **Collaborative Ideation –** Firstly, design sprints allow businesses to move away from a committee-based thinking process that can be cumbersome and tedious. With design sprints, the teams take a collaborative approach to arrive at a solution that considers ideas from various stakeholders.

- **Access to Stakeholders –** Design sprints also benefit agencies in getting to know their clients by helping them identify key stakeholders. This reduces approval time as the middlemen in the process can be pruned. Design sprints are goal-based with a clearly defined purpose, thus ensuring no time is wasted in identifying the final deliverable.

- **Effective Brainstorming –** Since each member of the design sprint committee is expected to come up with ideas, it can be viewed as an activity that encourages original thinking and experimentation. Team members can present their ideas without worrying about the execution part. The ideas thrown in together can be used in fragments to weave a possible solution to address the problem at hand.

- **Iterative User Feedback –** The final step in design sprints is user testing. The team's efforts are immediately acknowledged by validating ideas with prototypes and sketches. The feedback from this stage can be taken to tweak the solution further, thus reducing the cost of failure.

Making Design Sprints Work

The design sprint approach has two broad use cases – conceptualization and discovery.

- **Conceptualization Design Sprint –** A conceptualization design sprint can establish a new process or workflow. For instance, this design sprint is a good approach to elaborate a user journey upon app download. This approach allows the teams to think from the business point of view and run trials at the end of the sprint to get feedback.

- **Discovery Design Sprint –** The discovery design sprint methodology is applicable where a large project team is divided by job description. This process helps remove silos among departments and creates a collaborative environment by allowing various teams to interact and gather inputs to improve the development process. For instance, if the developers have created a new prototype for an app, other team members can be invited to review and share feedback on various aspects of the app. This works better than a focus group as each member is from a different core team, such as sales and marketing, each with their unique perspectives.

In the age of limited resources and tight budgets, businesses are looking at agile methods that would help them resolve issues without too much investment of time or money. Developed by Google, design sprints have been well received. While they cannot fully replace traditional design processes, they are certainly viewed as game changers especially where problem statements are well defined.

UNBOX is a UX practice at GS Lab | GAVS, where we design world-class yet practical digital experiences for our customers. In numerous engagements, we have been involved in various stages of the product development lifecycle, including PoCs and MVPs. Our experience in UX allows us to navigate vast domains and different customer segments easily. Unboxing user experience aspects at an early stage of the product surely does reap benefits later. You can find more information on our services here.

References

https://agilefirst.io/design-sprints/

https://medium.com/dallas-design-sprints/when-to-use-a-design-sprint-567afcc3653c

https://builtin.com/design-ux/design-sprint

About
the Author

Team UNBOX

U: Usability
N: Next Generation Media
B: Branding
O: Optimized Solutions
X: Experience

Unbox is a User Experience team at GS Lab | GAVS. The team prides itself on being the experience strategists who elevate their client's digital growth and add to their business value. Focus areas of the team being Branding, User Research, Visual Design and User Testing. Team has a mix of skills like Researcher, Information Architect, Interaction Designer, Brand Designer and Visual Designer. Team specializes in user research, working on new product concepts, redesign/revamp of existing products and feature enhancements. Team also helps in discovery phases involving UX for early product validation from business users. Agile collaboration with UI development teams to ensure the required product experience.

gslab | GAVS

EVERYTHING PRODUCT SERIES

Fireside Chat on Generative AI with AWS

Thursday, September 7, 2023

11:00 AM - 12:00 PM EST
08:30 PM - 09:30 IST

SPEAKERS

Giuseppe Zappia

GenAI Expert and Senior Solutions Architect, AWS

Randy DeFauw

GenAI Expert and Senior Principal Solutions Architect, AWS

Sameer Mahajan

Principal Architect, GS Lab | GAVS

In Episode 4 of our Everything Products series, we're delving into the captivating realm of Generative AI, its real-world applications and transformative impact, and we're thrilled to partner with AWS to bring you an insightful session.

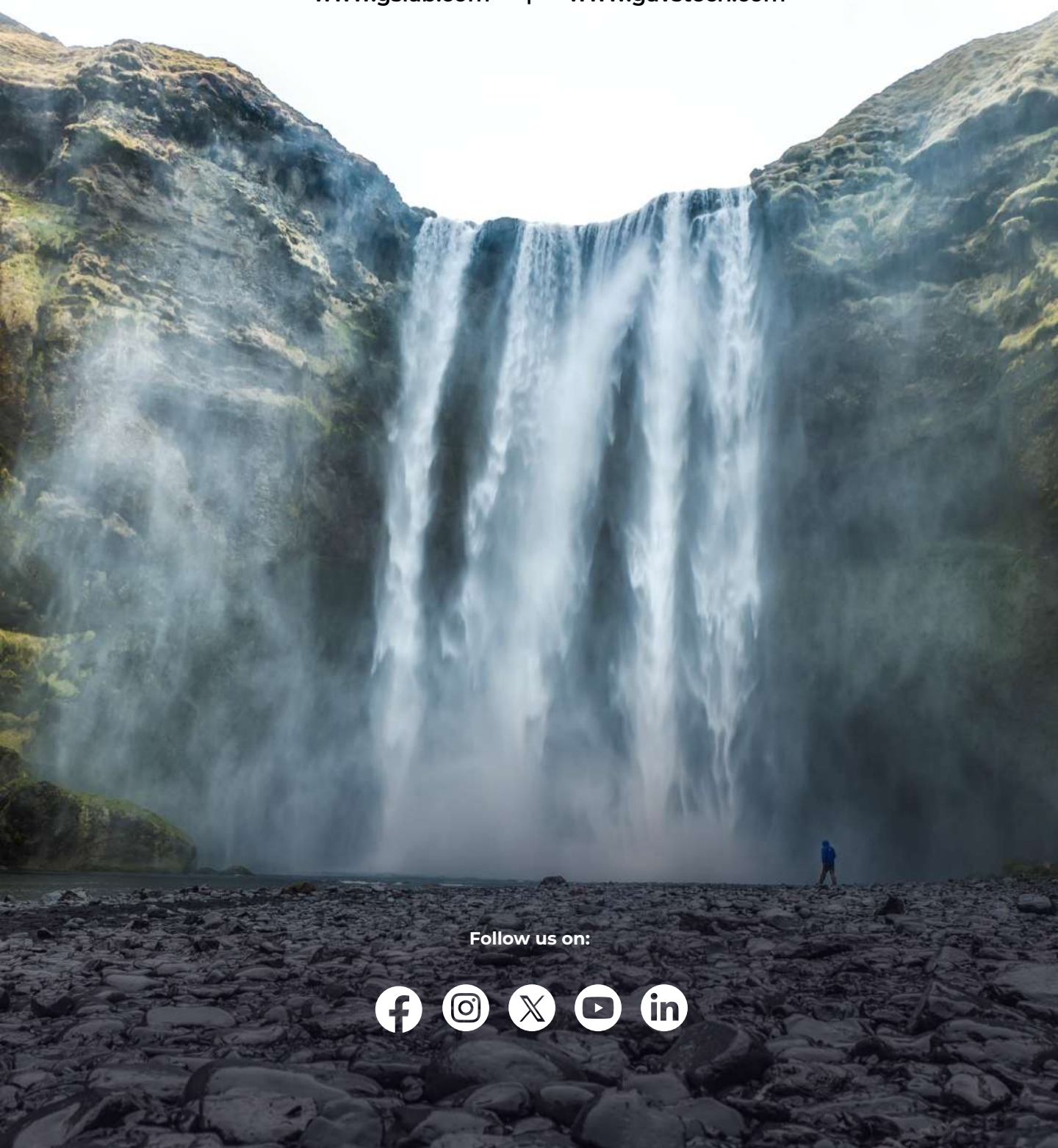
Our fireside chat format promises an intimate and insightful conversation about the incredible potential of Generative AI. In this episode, we will:

- **Demystify Generative AI:** Understand the core concepts and technologies driving Generative AI's capabilities.
- **Discuss Foundation Model vs ML Model.**
- **Explore Real-World Applications:** Discover how companies are using Generative AI to create art, compose music, generate content, design games, enhance healthcare, and more.
- **Dive into AWS Tools:** Get hands-on with AWS's suite of tools tailored for Generative AI.
- **Discuss different industries that explore Generative AI:** Delve into the industry use of Generative AI with areas such as Financial Services,
  Healthcare and Life Sciences, Automotive Manufacturing, Media and entertainment, Telecom, and Energy.
- **How Generative AI is changing the technology landscape.**
- **Discuss the potential of Generative AI.**

Register Now

enGAge

www.gslab.com | www.gavstech.com



Follow us on: