celerityx

BANKING ON A STRONG FOUNDATION:

PREVENTING THE NEXT DIGITAL TITANIC

Banking on a Strong Foundation

1.1 Overview of Digital Transformation in Banking
1.2 Importance of Modern Technology in the Banking Sector

The Titanic Analogy

2.1 Risks of Digital Transformation in Banking
2.2 Historical Case Studies
2.2.1 Uganda Cyber Attack
2.2.2 Bangladesh Central Bank Hack

Network Infrastructure in Banking

3.1 Importance of a Robust Network Infrastructure
3.2 Key Elements of a Banking Network Infrastructure
3.2.1 Affordability
3.2.2 Efficiency
3.2.3 Dependency
3.2.4 Standardization
3.2.5 Flexibility

Cybersecurity Threats

4.1 External and Internal Threats to Banking
4.2 Statistics and Case Studies on Cybersecurity Incidents
4.2.1 T-Mobile Data Breach
4.2.2 First American Financial Corporation Data Breach

Banking on a Strong Foundation:

5.1 Importance and Benefits of NLM in Banking
5.2 Key Areas of NLM
5.2.1 Fault Management
5.2.2 Configuration Management
5.2.3 Accounting Management
5.2.4 Performance Management
5.2.5 Security Management

Security Solutions

6.1 Multi-Layered Security Approach
6.2 CelerityX's OneX Solution for Banks
6.2.1 Key Features and Benefits

Conclusion

7.1 Summary of Cybersecurity Importance
7.2 Call to Action: Contact CelerityX for Customized Network Solutions

Banking on a Strong Foundation:
Preventing the Next Digital Titanic

The banking sector has undergone many changes to become more digitally driven. With the rapid breakthroughs in modern technologies, the Banking, Financial Services, and Insurance sectors have been experiencing tremendous digital transformations in recent years.

Digital transformation isn't a novel concept to the banking industry. However, it's gained immense popularity due to its ever-evolving changes in market and customer needs. Customers love convenience, and with the increasing competition, banks are continuously keeping an eye on these market-driven changes. Financial institutions are focusing on improving their digital services, such as launching new instant banking features on their mobile and Internet applications. This becomes an omnichannel strategy for banks used to remove all data barriers and enhance the customer journey.

Besides that, with the recent emergence of automation, banks are modernizing their strategies. With a growing demand for artificial intelligence (AI), blockchain, cloud computing, and the Internet of Things (IoT), these dominant technologies are streamlining banking operations and reducing the manual workload.

This digital shift is not just a trend but a necessity for survival in today's fast-paced world. Customers are looking to adopt digital strategies that help them manage their bank accounts with real-time transparency and security. Banks that don't align with trends are being left behind, like horse-drawn carriages in the age of cars.

However, as a coin has two sides, this sparkling digital world also has some unseen dangers lurking beneath the surface. Just as the Titanic's builders overlooked crucial safety measures, some banks might be rushing into digital transformation without a systemic approach.

The Titanic Analogy:

A Massive Ship with Unseen Dangers Below the Surface

The Titanic was hailed as unsinkable. It was the pride of its time, much like how some banks view their digital offerings today. However, we all know how that story ended. Just as the Titanic's crew couldn't see the iceberg until it was too late, banks might not notice the flaws in their digital infrastructure until a crisis hits. That means a single glitch could sink customer trust faster than you can say, "System error."

For instance, if it's a payday and millions of people try to access their accounts at once, the bank's systems shut down under the load, and your screen displays, "Sorry, we're experiencing technical difficulties." This single error could impact the operations of many companies that are dependent on your services.

For instance, in Uganda, the cyber attack of October 2020 affected the country's largest mobile money networks, MTN and Airtel. This resulted in a major four-day disruption of service transactions.

These problems related to downtime can be resolved, but what if your bank becomes a victim of a data breach or cyber security attack due to issues in network security? This can massively damage your reputation in the market.

This is a worldwide problem. For instance, in February 2016, a group of hackers targeted the Central Bank of Bangladesh. The hackers tried to steal $1 billion by exploiting the vulnerabilities in SWIFT, the global financial system's primary electronic payment messaging system. Most of the transactions were blocked, but $101 million was still missing.

This type of heist was a wake-up call for financial institutions, who needed to understand that cyber attacks were underestimated in their systems.

The Importance of a Robust Network Infrastructure For Banking Operations

A bank's network infrastructure is like the hull of a ship. From effective communication to improving security and a top-notch customer experience, a robust network infrastructure is capable of performing banking functions. This hull comprises servers, routers, wireless access, cables, data centers, cybersecurity measures, and more.

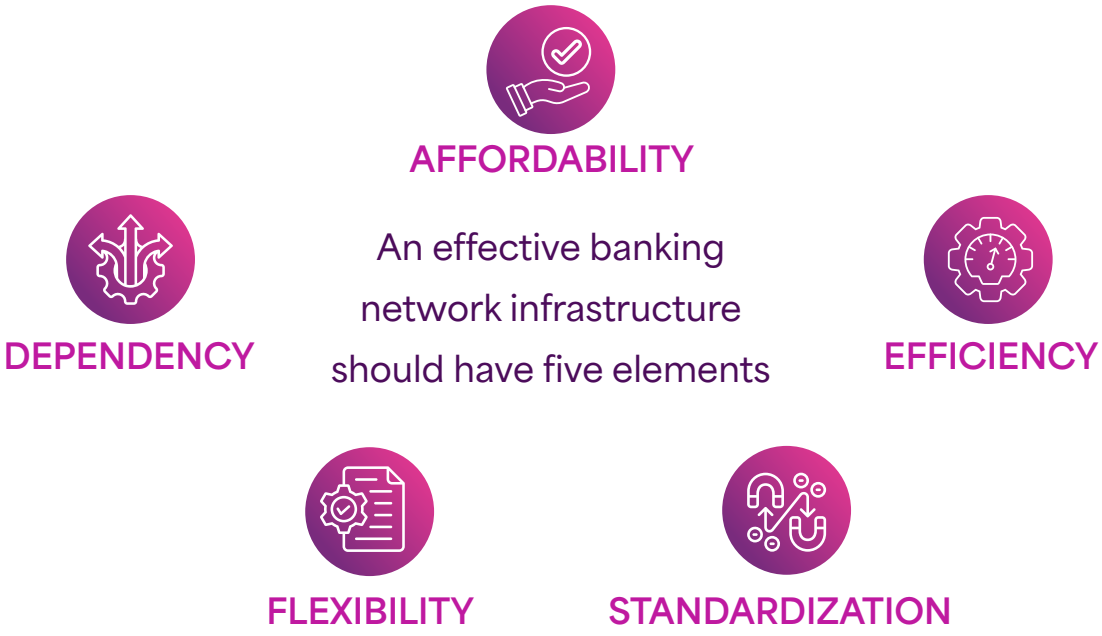
As banks sail into the digital future, they must remember the lessons of the Titanic. It's not enough to be big and impressive; you have to be prepared for the unexpected. A well-designed network infrastructure serves as the backbone that creates multiple layers of security, providing a shield against cyber threats (data breaches, hacking, and phishing) and encryption, safeguarding customer-sensitive data.

Moreover, a robust network infrastructure in the banking sector enables quick and easy transaction processing with real-time data access that minimizes waiting time and improves overall operational efficiency.

Building a Strong Hull:

A Bank's Network Infrastructure

A bank's infrastructure includes a system of hardware, software, facilities, service, and network components designed to support the delivery of business systems and IT-enabled processes.



While improving the network infrastructure, it is essential to consider the affordability factor. Moving away from legacy systems can help you save a ton of money rather than depending upon old and traditional systems. However, rather than just considering the present cost of implementation, think of the infrastructure's long-term use. With new and evolving technologies, it is best to invest in a dynamic infrastructure that can adapt to new modifications easily without incurring a significant cost.

Also, the infrastructure should focus on making the operations more efficient and better. For instance, it is best to avoid technologies that have a steeper learning curve, no matter how advanced they are. If your employees find it hard to work with advanced systems, it will definitely make the investment more expensive.

Banking IT infrastructure is a complex network that integrates branches, ATMs, and data centers. These are fast-paced business environments and support mission-critical processes, which include transactional, compliance, and relationship-building components.

Hence, you require a dependable infrastructure with negligible downtime, robust security functions, and high connectivity, such that updates are reflected in real time. A robust and dynamic network infrastructure ensures that it can manage a high volume of transactions daily.

Standardizing helps set the baseline of standards that fit your business strategy, security policies, and goals. This will help reduce complexities and ensure cost savings through economies of scale, ease of integration, improved efficiency, and better IT support.

This will also help banks choose the right solutions and simplify vendor management processes because all these solutions are aligned to ensure compatibility and interoperability for customers.

When one element goes out of the picture, the result is network outages. For instance, prominent banks, like DBS and Citibank, experienced network outages in Singapore when the Equinix Chiller upgrade did not go as planned. The outage happened in the afternoon of October 14, and it wasn't fully recovered until the morning of the next day.

The reason behind the outage was that the cooling systems at an Equnix data center were either offline or degraded due to upgrade work. This raised temperatures in some data halls and caused the equipment to shut down. Both banks had activated backup sites, but they weren't able to fully recover their services.

In cases like this related to network outages, it is best to wait for resolution rather than turning to backup. This is especially applicable when the issues are known to resolve quickly compared to the time required to launch the backup. However, sometimes, it is best to switch to backup to restore the services.

Hence, it is best to know the cause of the issue and then make a well-informed decision to avoid extended delays and downtime.

Icebergs Ahead:
Cybersecurity Threats

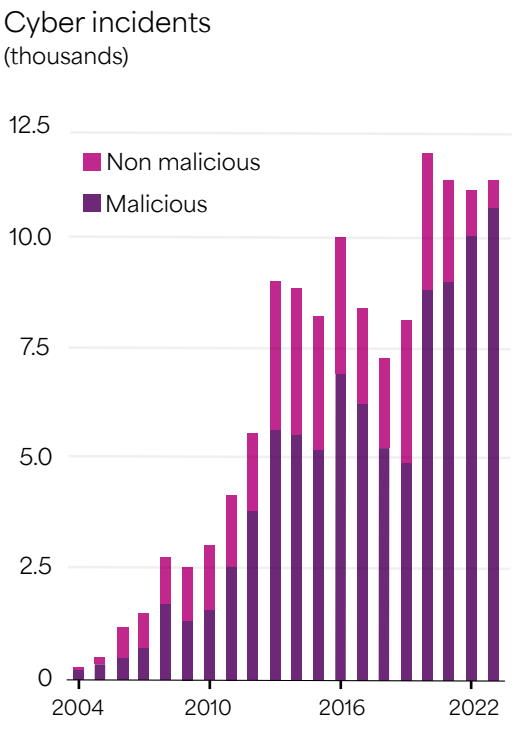
There are primarily two types of threats that a bank may encounter, including:

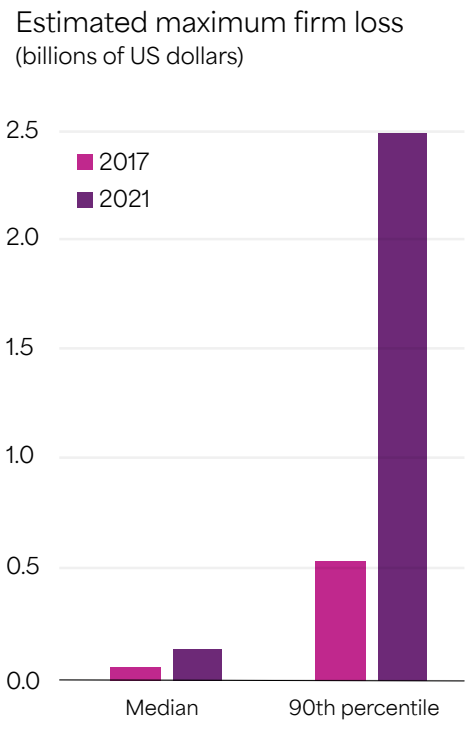
External threats originate from outside the bank and gain unauthorized access to customer-sensitive data. These usually include malware attacks, phishing attacks, DDoS attacks, and so on.

Internal threats are those that arise within the banking system. They include insider attacks, accidental data breaches, privilege abuse, and more.

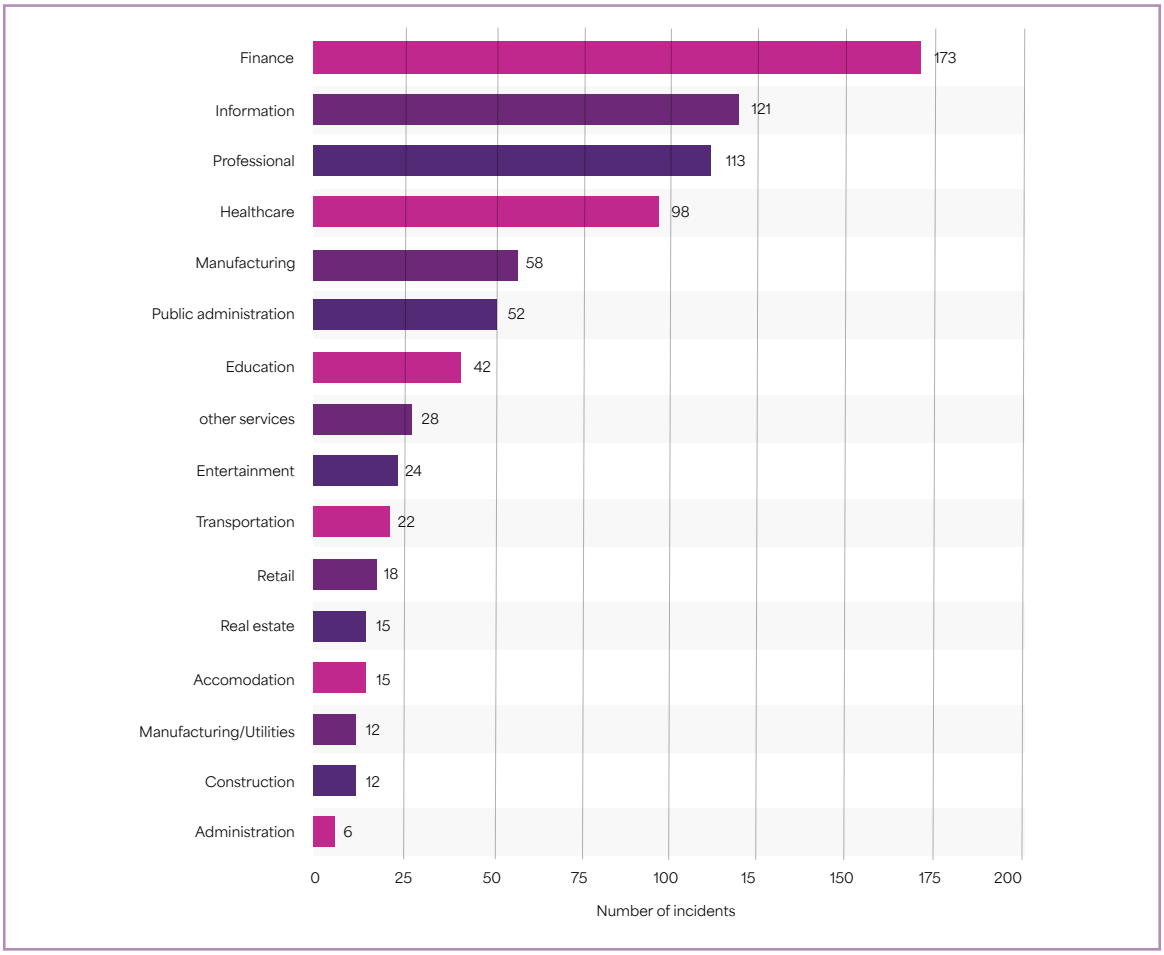
Banks hold money and customers' sensitive data. However, nowadays, banks are the most targeted sectors by cyber attackers, resulting in data breaches. Data breaches have become a significant concern for financial institutions and customers alike, resulting in major financial and reputational losses.

Global industry sectors most targeted by basic web application attacks from November 2021 to October 2022





According to IMF reports, one-fifth of the reported cyber incidents have affected the global financial sector in the past two decades. This has caused financial firms direct losses of $12 billion. Besides, since 2020, the direct losses have been reported to be around $2.5 billion.



Despite leveraging robust data security systems, cyber attackers are continually finding new ways to gain unauthorized access to valuable customer data and credentials. According to the Statista report, a major data breach in the financial industry was noticed in 2019 in the US at First American Financial Corporation. It caused the leakage of around 885 million financial and personal records.

The rise of AI attacks, where cyber attackers leverage AI to hack systems and steal information. According to a Georgetown Center for Security and Emerging Technology 2020 report, machine learning has the potential to increase the scale and success rate of social engineering and spear phishing attacks.

Harvard Business Review reported that around 60% of participants fell prey to AI-automated phishing attacks compared to non-AI phishing attacks. LLMs can automate phishing attacks, reducing the costs by more than 95% and achieving equal or greater success rates.

Besides that, there are many ways that AI can be used to breach data security and network infrastructure.

Hackers can use Gen AI tools to generate false emails, attachments, and emails to entice unaware employees, and they fall prey to clicking the compromised links and entering their crucial details.

Besides, AI can be used to detect anomalies or vulnerabilities in a system in less time than manually finding the flaw within the lines of code. This can be achieved by reversing the comparisons between the published version of the software to find out what has been patched, or it can be done by analyzing the open-source code as well.

Gen AI can be used to create polymorphic malware that adapts and mutates the source code. This allows the malware to remain undetected, and security protocols, like traditional antivirus, use signature-based identification.

AI can make brute-force attacks easy to conduct, as it can assist in automating them and allow hackers to analyze user behavior to figure out passwords easily.

There are AI tools that can actively record the different keys that the user types in their keywords to guess the passwords with 95% accuracy.

There is a Deep Fake AI hacking tactic where hackers use Gen AI to create fake videos that impersonate a particular person or environment, tricking the victim into believing that it is real. Deepfakes can affect anyone, and according to the World Economic Forum, around 66% of cybersecurity experts have experienced deepfake attacks within their organization in 2022.

Besides, prominent companies and organizations have already become victims of AI hacking. For instance, in 2018, IKEA's well-known online marketplace TaskRabbit was targeted, and over 3.75 million records of Taskers and Clients were affected.

TaskRabbit is a platform that operates on a large scale, and it helps in aligning freelancers with clients to complete tasks related to housekeeping, moving, delivery, and similar industries. However, due to the breach, personal information and financial information were stolen. As the company dealt with the blow, the website and app had to be taken down for a while. According to investigations, this was a **Distributed Denial of Service (DDoS) attack,** and the culprit was an AI-enabled botnet.

In another case, T-Mobile, a renowned wireless network operator that has survived nine separate cyber attacks within the past five years, faced a cyber attack again in 2023. T-Mobile disclosed that a data breach affected the data of over **37 million** of its customers, specifically prepaid and subscription consumers.

According to the company's investigations, the hackers had access to an **API (application programming interface)** with AI capabilities for over 6 weeks. As per their 8-K Sec filing, the hackers first retrieved data through the API around 25 November 2022. This indicates that this API data breach had a dwell time of over 40 days.

The company has mentioned that the unauthorized API access exposed customer information, such as names, emails, phone numbers, and birthdates, along with the number of lines on the account and service plan features. **Customers' social security numbers, Government IDs, credit card information, and PINs weren't exposed**.

For those who are unversed, an API breach happens when bad actors get access to the system through a compromised API. It can happen when the security-protecting API is compromised, manipulated, or insufficient to allow malicious elements to exploit the IT systems. The reasons can be weak authentication, insufficient encryption, insecure endpoints, improper key management, or poor API logic. Besides, it could also happen when there is a lack of visibility to overview the organization's API inventory, called unmanageable API sprawl.

When we look at the consequences of these kinds of critical incidents of data breaches, the repercussions are more impactful than we can imagine. These breaches raise questions beyond just cyber security but result in **financial loss, reputational damage, regulatory fines, legal troubles, and loss of customer trust**.

Customers rely on banks to secure their sensitive financial data and protect their accounts from unauthorized access. However, when a data breach occurs, it can result in a loss of trust among customers and negative repercussions for banks. If customers perceive that banks can't safeguard their financial information, they may not feel comfortable using their accounts or making transactions. This may lead to a significant decrease in customer satisfaction and a lack of trust in the specific bank, forcing them to look for alternative banking options.

Navigating the Waters:
Network Lifecycle Management

Banks proactively need to invest in robust and highly advanced IT practices to monitor the deployed infrastructure for optimal performance and minimal flaws. Hence, network lifecycle management (NLM) comes into play, which refers to designing and implementing a comprehensive strategy to overview the entire network lifespan from design to deployment and operation.

The NLM is a dynamic strategy that ensures that the established network infrastructure meets the evolving needs of the organization in terms of performance, security, capacity, and technological advancements. Here's how NLM benefits banking organizations:

Effective network lifecycle management ensures high network performance and reliability because regular maintenance and updates, including patchwork, make things run smoothly.

NLM focuses on detecting errors and flaws. Once the issues are highlighted, they can be solved easily. Hence, NLM improves network security by promptly addressing the detected vulnerabilities.

Optimizing the network's performance helps in extending its lifespan and reduces the need to go for full-scale hardware replacements.

NLM allows organizations to scale and adopt new technologies without any major overhauls.

However, how does network lifecycle management ensure all the benefits? This is because network lifecycle management is categorized into five key areas, which are:


Fault Management


Configuration Management


Accounting Management


Performance Management


Security Management

These disciplines are interconnected and assist in detecting and addressing potential network problems before they could disrupt business operations. Here's how each discipline helps in ensuring consistency in operations:

Fault Management

Fault Management is responsible for addressing errors promptly, minimizing disruptions to the network, and ensuring optimal performance. This helps maintain high uptime by resolving network issues, like slow internet speeds, weak WiFi signals, IP address conflicts due to incorrect configurations, and potential hardware failure, like loose cables.

Configuration Management

Configuration management plays a major role in network management. It primarily focuses on effective change management, automating repetitive tasks, and tracking all versions of network configurations.

Accounting management

Accounting management monitors network usage, regulates network resources, implements control measures, and tracks user-specific actions for cost allocation.

Performance management

Performance management tracks and ensures that the network is optimized to deliver smooth performance. It considers factors such as bottleneck latency rates, throughput capacity, jitter fluctuations, reordering tendencies, and potential packet loss.

Security management

Security management constantly monitors the network for potential breaches and enforcement of policies to create a secure network environment.

NetX, one of CelerityX's products, is an efficient network management tool designed and tailored for the needs of enterprise networking. Here's how NetX is a perfect NLM solution for your banking infrastructure:

NetX provides a centralized platform for streamlined procurement and management of vendors.

It offers Proactive monitoring to boost efficiency and productivity.

From the chains of unreliable connections and helps you create an environment with almost negligible downtime due to issues.

Banco del Pacifico, one of Ecuador's leading state financial institutions, overcomes challenges such as server instability, slow-loading databases, fragmented data management, and limited scalability with the help of a robust NLM solution.

Avoiding Collision:
Security Solutions

Network Lifecycle Management helps in future-proofing the IT infrastructure and network, but what about the increasing endpoints? With the rise in digitalization, the number of endpoints of any organization is increasing, and these endpoints become risky to jeopardize the entire endpoint. To ensure maximum security and safety, it is essential to tie up all the endpoints.

Centralized solutions are no longer sufficient to protect networks; rather, they require multi-layered security solutions to reduce exposure to security breaches. Endpoint security solutions implement a multi-layered approach that blocks errors and secures endpoints. These solutions mirror improvised systems with firewalls, access controls, and vulnerability assessments to neutralize threats.

CelerityX offers OneX, a Comprehensive & Tested Solution for Banks
all-in-one solution for enhanced network security. Replace multiple devices and ensure reliable connectivity across wireless and wired networks for your retail operations.

OneX prioritizes application and user-level traffic, guaranteeing 100% uptime for CCTV, core banking, and POS applications. It includes built-in Unified Threat Management (UTM) features like a stateful firewall, IDS/IPS, and endpoint security, eliminating the need for multiple devices.

Providing proof is essential, and hence, organizations should document their ability as a team to control risks and protect sensitive information. This helps reduce the chances of any regulatory fines because you have met all the compliance requirements as set by the industry. Also, organizations can opt for a SOC 2 report that provides support documentation for sufficient endpoint security.

The Bottom Line,

Nowadays, cybersecurity is no longer a secondary aspect; in fact, it is a foundational pillar in strengthening the relationship with customers. While protecting critical money-related data, banks are responsible for safely securing customer data, such as phone numbers, Government IDs, and more.

Whether it is a security breach or a never-seen-before glitch incident, banks' reputations might get hampered because of any of the issues. That's why it is essential to understand that banking organizations and financial institutions should invest in monitoring their network infrastructure and switch to a holistic enterprise-grade network.

CelerityX allows banking institutions to choose from a variety of network solutions, like high-speed broadband,Dedicated Internet leased line, highly-secured SD-WAN (OneX), P2P Link, Internet Leased Lines, Multi-Protocol Label Switching, and Broadband Over Satellite (SkyX).

We can assist in designing and deploying a customized network solution designed to meet the evolving needs of businesses to remain highly available, improve uptimes, and secure a network environment. Contact our experts and tell us your issues. We will help you understand your problems and provide the best solution that aligns with your current and future needs.

Cutting edge networks and digital solutions

NetX
Always on. Always connected.

Your one stop hub for seamless WAN connectivity solutions.

SkyX
Pervasive community, anywhere.

High speed satellite broadband for remote connectivity.

OneX
Your WAN. Your way.

The ultimate all-in-one security solution for your business locations.

HomeX
Connect. Collaborate. Conquer

Boost remote connectivity with smart features.

- Speed in Support and Service
- Speed in Trouble Ticket Solution
- Speed in Solutioning and Proof of Concept
- Speed in Project Management

www.celerityx.com

4th Top Private ISPs	**10000+** Partners	**300+** Cities	Up to **1000 Mbps** One Gigafiber	**1 Million** retail customers	**>5000** Enterprises	**Leading provider** of broadband over satellite across India