Key Take Aways from Maleny/Montville Chamber Business Breakfast with Telstra

1. *Mobile Network Traffic was the main underlying factor Telstra highlighted as behind the reliability issues for the mobile network. It was the reason for bringing forward the recent upgrades, to expand capacity.*

It would be interesting to ask if Telstra can share their mobile network analysis for the members to visualise and see, along with predictions for how the upgrades should improve reliability. This could be followed by 6 monthly updates of the data to see the forecast improvement is realised.

2. *Telstra strongly encouraged creating redundancy in business digital comm systems via use of the NBN.*

Is it possible to contact the NBN (perhaps via Andrew Fisher) to get demographic data for our region as to uptake – how many fibre connections and wireless NBN connections (I don't know who would have the data on uptake of satellite internet like Starlink). You could cross reference this data with a survey of members to see which services they are using, and also which ones they cannot access.

And again it would be interesting if NBN can provide uptime and capacity analysis for each of their networks (fibre and wireless), and indicate what the reason was for the recent wireless NBN outages around Montville (and Maleny if they occurred too).

3. *It appeared to me listening to the conversation, that we have an issue from both the Telstra perspective and the business perspective, of "unknown-knowns".*

Telstra doesn't seem to be aware of the unique service access issues across the hinterland due to topography, or understand the nature of most hinterland businesses (i.e. small business, who perhaps run very tight for cash flow and just cant afford to miss key sale periods, or lose repeat customers due to poor connectivity issues). Also their regional liason officer role has a huge territory so getting deeply connected and aware of things like which major event is when on the hinterland, is going to be very challenging.

And perhaps there are unknown-knowns with the members about the ways the communication systems (mobile and internet) are run, what risks they present to the business, and different options to manage those risks. Missing stakeholders from the conversation are NBN, IT service providers to business, and satellite internet companies (starlink).

This part got me thinking and I did a quick bit of research which you are welcome to share with your members – Ive been sharing it on Linkedin to my network as a key sustainability theme i.e. how to keep your business resilient in a digital world.

What are the risks for businesses that rely on digital communication tools like mobile networks and the internet to operate?

Businesses that heavily rely on digital communication tools like mobile networks and the internet to operate are exposed to various risks. Some of the key risks include:

Connectivity Issues:

Reliance on mobile networks and the internet makes businesses vulnerable to connectivity issues. Network outages, hardware failures, or disruptions in service can result in loss of communication, interrupted operations, and reduced productivity.

Cybersecurity Threats:

Increased digital connectivity exposes businesses to cybersecurity threats such as data breaches, hacking, malware, and phishing attacks. These threats can lead to financial losses, damage to reputation, compromised customer data, and potential legal consequences.

Data Loss or Corruption:

Storing critical business data and information in digital formats introduces the risk of data loss or corruption. Technical failures, malware attacks, or human error can lead to data breaches or loss, resulting in significant operational disruptions and potential legal liabilities.

Privacy Concerns:

Businesses that rely on digital communication tools must handle sensitive customer and employee data. Failure to protect privacy can result in breaches of confidentiality, loss of trust, regulatory penalties, and reputational damage.

Dependency on Service Providers:

Businesses rely on third-party service providers for mobile networks and internet connectivity. Any disruptions or issues with these providers, such as service outages or contractual disputes, can significantly impact business operations.

Systemic Risks:

The complex nature of digital communication systems exposes businesses to systemic risks, such as widespread cyberattacks or infrastructure failures. These events can disrupt the functioning of entire industries, affecting business continuity and recovery.

Regulatory and Legal Compliance:

Businesses operating in digital environments must comply with various laws and regulations governing data protection, privacy, and cybersecurity. Non-compliance can result in legal actions, fines, reputational damage, and loss of customer trust.

Technological Obsolescence:

Rapid advancements in technology can render existing digital communication tools obsolete. Businesses need to stay updated with the latest technologies and invest in regular upgrades to remain competitive and ensure compatibility with evolving digital infrastructure.

To mitigate these risks, businesses should adopt robust cybersecurity measures, implement backup and disaster recovery plans, regularly update and patch software, train employees on cybersecurity best practices, and stay informed about emerging threats and regulatory requirements. Diversifying connectivity options and establishing contingency plans can also help minimize the impact of connectivity issues.

What the best controls businesses can implement to manage the risks of connectivity issues

To manage the risks associated with connectivity issues, businesses can implement several controls. Here are some of the best controls to consider:

Redundant Connectivity:
Establish redundant connections from multiple service providers to ensure uninterrupted connectivity. This could involve having backup internet connections from different providers or utilizing alternative technologies like cellular networks as a backup.

Service Level Agreements (SLAs):
When engaging with service providers, negotiate SLAs that include uptime guarantees, response times, and penalties for service disruptions. Ensure that the SLAs align with your business requirements and provide adequate compensation for downtime.

Network Monitoring and Alerting:
Implement network monitoring tools that continuously monitor the health and performance of your network infrastructure. These tools can provide real-time alerts for connectivity issues, allowing your IT team to address them promptly.

Backup Power Systems:
Install uninterruptible power supply (UPS) units or backup generators to ensure continued power supply during outages. This helps maintain critical network equipment, such as routers and switches, and prevents disruption due to power failures.

Cloud-Based Services:
Leverage cloud-based services and platforms that have built-in redundancy and failover mechanisms. By distributing your services across multiple data centers, you can minimize the impact of localized connectivity issues.

Disaster Recovery Planning:
Develop a comprehensive disaster recovery plan that outlines procedures for addressing connectivity disruptions. This plan should include backup data centers, alternative communication channels, and steps for quickly restoring operations in the event of a network failure.

Business Continuity Planning:
Incorporate connectivity risks into your broader business continuity plan. Identify critical functions and prioritize their restoration during connectivity outages. Establish alternative work arrangements, such as remote work options, to ensure operational continuity.

Testing and Maintenance:

Regularly test and maintain your network infrastructure to identify potential vulnerabilities or points of failure. Conduct network resilience tests to assess the ability of your systems to withstand connectivity disruptions and recover swiftly.

Incident Response and Escalation:
Define clear incident response procedures that outline the steps to be taken in the event of a connectivity issue. Establish communication channels and escalation paths to ensure that incidents are promptly reported, investigated, and resolved.

Employee Training and Awareness:
Educate your employees about the potential risks of connectivity issues and how to respond to them. Provide training on basic troubleshooting techniques, reporting procedures, and the importance of backup and contingency plans.

By implementing these controls, businesses can minimize the impact of connectivity issues and ensure that critical operations can continue even in the face of disruptions. Regular monitoring, testing, and proactive measures will enhance the resilience of your network infrastructure and maintain business continuity.

Do these control change if the business is a sole trader or small business?

The controls mentioned earlier can be adapted for sole traders and small businesses to suit their specific needs and resources. Here are some considerations for implementing these controls in a sole trader or small business context:

Redundant Connectivity:
While having multiple service providers might not be feasible for all sole traders or small businesses, exploring alternative options such as mobile hotspot devices or utilizing public Wi-Fi networks as backup connectivity can be more cost-effective.

Service Level Agreements (SLAs):
While negotiating SLAs may be more challenging for smaller businesses, it's still important to assess and compare the service levels offered by different providers. Look for providers that offer reliable connectivity and responsive customer support within your budget constraints.

Network Monitoring and Alerting:
Seek out affordable or free network monitoring tools tailored for smaller networks. Many cloud-based monitoring solutions offer flexible pricing models based on the scale of your network infrastructure.

Backup Power Systems:
Consider investing in smaller-scale UPS units that can provide power to essential networking equipment during short outages. This helps maintain connectivity for critical operations even during brief power disruptions.

Cloud-Based Services:

Leverage cost-effective cloud-based services that provide built-in redundancy and failover capabilities. Small businesses can benefit from using Software-as-a-Service (SaaS) solutions that offload infrastructure management and ensure high availability.

Disaster Recovery Planning:
While small businesses may not have dedicated backup data centers, they can leverage cloud storage or affordable off-site backup services to store critical data. Develop a disaster recovery plan that focuses on quickly restoring essential operations and data access.

Business Continuity Planning:
Tailor your business continuity plan to the specific needs and scale of your business. Identify critical functions and prioritize their restoration during disruptions. Consider alternative work arrangements, such as remote work or shared office spaces, to ensure operational continuity.

Testing and Maintenance:
Regularly assess the health of your network infrastructure by conducting basic testing and maintenance tasks, even if it involves manual checks and updates. Prioritize essential security updates and patches to mitigate vulnerabilities.

Incident Response and Escalation:
Establish clear incident response procedures and communication channels that align with the size and structure of your business. Designate specific roles or responsibilities to individuals or external vendors who can assist during connectivity issues.

Employee Training and Awareness:
Provide basic training and awareness sessions for your employees to understand the importance of connectivity and backup plans. Emphasize the role of individuals in reporting connectivity issues promptly and following prescribed procedures.

It's essential for sole traders and small businesses to balance their needs and available resources when implementing these controls. Prioritize the controls that align with your budget, scalability, and risk tolerance, and seek cost-effective solutions that offer the most significant impact for your business's continuity and connectivity.

What existing technology allows private enterprises to use an internet connection to provide connectivity for mobile phones from the business network to public mobile coverage networks

There are technologies available that allow private enterprises to provide connectivity for mobile phones using their business internet network to access public mobile coverage networks. One such technology is called a femtocell or a small cell.

A femtocell is a small cellular base station that connects to the business's internet connection. It creates a localized cell coverage area within the business premises, allowing mobile phones to connect to the business network and utilize the internet connection for voice and data services. The femtocell then routes the mobile traffic through the business's internet connection to the public mobile network.

By deploying femtocells, businesses can provide enhanced cellular coverage and connectivity within their premises, which can be particularly beneficial in areas with weak cellular signals or in buildings with poor reception. It enables employees, customers, or visitors to use their mobile devices without relying solely on the public mobile coverage network.

Femtocells are typically provided by mobile network operators or specialized equipment vendors. They require proper configuration, integration with the existing network infrastructure, and coordination with the mobile network operator to ensure compatibility and proper functioning.

It's worth noting that the availability and specific implementation of femtocells may vary depending on the mobile network operator and the region. Businesses interested in deploying femtocells should consult with their preferred mobile network operator or equipment vendors to determine the feasibility and requirements for implementing such a solution.

UPDATE : I haven't been able to find a provider for femtocells in Queensland as yet – maybe an opportunity to speak with some IT guru's to get their understanding, as well as aksing Telstra of course (they used to offer them but have retracted from the market)

What would be the top 3 best controls a small business can use to manage the risks of digital communication tools

For a small business, here are three of the best controls to manage the risks associated with digital communication tools:

Robust Cybersecurity Measures:
Implement strong cybersecurity measures to protect against data breaches, malware, and other cyber threats. This includes installing and regularly updating antivirus software, using firewalls, enabling secure password practices, and implementing encryption for sensitive data. Regular security assessments and employee training on cybersecurity best practices are also crucial.

Regular Data Backups and Disaster Recovery Planning:
Regularly back up critical business data and establish a disaster recovery plan. This involves storing data backups in secure off-site or cloud locations, conducting regular backup tests to ensure data integrity, and documenting procedures for recovering data and systems in the event of a disruption or loss. Backup data should be easily accessible and regularly tested to ensure its effectiveness.

Contractual Agreements and Vendor Due Diligence:
When working with service providers or using digital communication tools, carefully review and negotiate contractual agreements that address privacy, security, and service levels. Perform due diligence on vendors to ensure they have strong security practices and comply with relevant regulations. This includes assessing their security certifications, reputation, and history of incidents.

Implementing these controls helps mitigate some of the most significant risks associated with digital communication tools for small businesses. By focusing on cybersecurity, data backup and recovery, and vendor diligence, businesses can enhance their security posture and protect their critical digital assets.