"A Comprehensive Approach to Cyber Resilience" by Chon Abraham is a discussion of the importance of cyber resilience in today's digital age. Cyber resilience refers to an organization’s ability to recover from and adapt to cyber threats and attacks. In the article, Abraham argues that cyber resilience is critical for the success of any organization, as it allows them to continue to operate and function effectively in the face of cyber threats.

Abraham notes that a comprehensive approach to cyber resilience involves a number of different elements, including strong security protocols, effective incident response planning, and the ability to recover quickly from a cyber attack. He also emphasizes the importance of training and education for employees in order to help prevent cyber attacks from occurring in the first place.

To develop a comprehensive approach to cyber resilience, Abraham suggests that organizations take the following steps:

1. Assess the organization's current level of cyber resilience and identify any areas that need improvement. This may involve conducting a risk assessment to identify potential vulnerabilities and determining the likelihood and impact of a cyber-attack.
2. Develop a plan for responding to cyber attacks, including the identification of key personnel and resources that will be needed to recover from an attack. The plan should outline the steps that need to be taken in the event of a cyber attack, including how to communicate with employees and stakeholders, secure the affected systems, and restore operations.
3. Implement strong security protocols to prevent cyber attacks from occurring in the first place. This may include measures such as firewall protection, antivirus software, and employee training. It may also involve implementing additional security measures, such as two-factor authentication or encryption, to further protect sensitive data.
4. Conduct regular tests and drills to ensure that the organization's cyber resilience plans are effective. This may involve simulated cyber-attacks or other exercises to test the organization's ability to respond to a real-world cyber threat.
5. Monitor the organization's systems and networks to detect any potential threats and take appropriate action to prevent or mitigate them. This may involve implementing monitoring tools or hiring a dedicated cybersecurity team to monitor for potential threats.

Overall, "A Comprehensive Approach to Cyber Resilience" is a useful resource for organizations looking to improve their cyber resilience and protect themselves from cyber threats. It highlights the importance of a proactive approach to cybersecurity and the need for a comprehensive plan to respond to cyber-attacks. By following the steps outlined in the article, organizations can improve their ability to recover from and adapt to cyber threats, helping to ensure their continued success and longevity.