Podcast Script for Cyber Security: The Home is Still the Office and New Services in Times of Crisis.

PRACTICE AREA: **Cyber Security**
HOST NAME: **None**
GUEST NAME: Syam Thommandru

1. The COVID-19 pandemic and the resulting rapid adoption of remote working arrangements and technologies present new and increased cybersecurity risks for organizations of all kinds and sizes.
2. A confluence of trends – including ever-mounting cyber attacks, expanding network attack surfaces stopping from increased teleworking during the pandemic, and an enduring shortage of skilled cybersecurity workforce talent – is creating demand for more sovereign cybersecurity technologies and services
3. Now that the initial scramble to get employees up and running from home—including investments in cloud service, video conferencing platforms and collaboration tools—is over, it's time to rethink security policies when it comes to the risks that organizations are willing to take.
4. This also includes how staff is trained to handle emerging cyber-threats related to COVID-19.
5. it's all about organizations' data, who can access it, and how it must be protected and secured going forward.
6. These are the types of conversations that CSOs and CISOs are having about the risks their organizations face in a permanent work-from-home world and how cybersecurity policies need updating to reflect that.
7. What has happened in the current situation is that we know we can access stuff in the cloud, but a real concern for security people is around the way in which that data is then being accessed, and how do I secure that effectively,"
8. "We've now got all of these people working from [remote] locations, and frankly, we can't necessarily always assure ourselves of the security from those locations."
9. Many organizations are using tools to secure the employee's endpoint. But in parallel, working from home increased the already growing trend of BYOD – connecting personal devices to the organization network. Working from home means the devices are also connected to non-corporate networks (mostly the home network), with other devices that are entirely out of reach for the organization's IT department and policies.
10. These devices are inherently less secure – other family devices, IoT devices, ISP's routers, and others that are out of the control of the company. Many employees are also sharing their devices with family members, who are sometimes less technology-oriented and less familiar with cyber hygiene. And last, from a physical security perspective, it is usually easier to break into houses than to offices.
11. To handle this BYOD and remote work trend, endpoint security should be enforced to protect the organization owned devices as much as possible. Still, it has to be combined with a zero-trust approach, multi-factor-authentication (MFA), and training (log out from organization accounts on devices, etc.).

12. New Services in Times of Crisis
13. When the world is changing, our technology needs change with it. New features are added to products, new sub-portals are added to portals, and the changes need to happen ASAP – every day counts.
14. In parallel, the workforce is remote and is, in general, less physically available than before. It is important to remember that while rushing to the release of a new version or feature, one cannot overlook cybersecurity aspects.
15. The risks are high when trying to finish things quickly, and we have to control the rush of the version release and take (even a little) time to consider where things can go wrong and prevent them from getting there early in the development process.
16. To summarize, many things have changed in the last few months, including the way we work and consume our internet traffic.
17. The cybersecurity industry should react to these changes in order to continue securing organizations and people. On top of the reaction aspects, the changes should also start a discussion of longer-term strategic moves,