Track: Future-Proof Information Security

Challenge Four

The Borderless Office

The Core Problem

Employees now work from anywhere, using personal devices and home networks. The old model of a secure corporate "castle" with a VPN "moat" is broken. Company data is now everywhere.

- **The Big Question: How might we (organizations) secure their sensitive data and corporate systems in a "work from anywhere" world, without compromising employee productivity or user experience?**

- **Spark Questions:**

- What if they assumed their network was already compromised and secured the data itself (a "zero-trust" approach)?
- How can we verify the user, their device, and their context before granting access?
- How should banks be protected without making life difficult for their employees?

Context

The shift to telecommuting presents significant challenges in maintaining information security. Employees now access confidential company information from everywhere, often using their personal devices and unsecured networks. These vulnerabilities open employees and businesses to threats such as phishing, malware, and unauthorized access to corporate systems. Traditional security solutions, including firewalls and VPNs, fall short in protecting against distributed workforces.

In addition, the lack of physical oversight in remote settings makes it harder to enforce security policies, such as strong password practices or regular software updates. Employees may also inadvertently expose sensitive information by using unapproved applications or cloud services. This problem is further compounded by the increasing sophistication of cyberattacks targeting remote workers.

How can we create a seamless yet secure remote work ecosystem that adapts to the evolving threat landscape?