Remote Workforce Remains at the Forefront of Cyberattacks

More than 1,300 security leaders, business executives and remote employees took part in a survey conducted by Forrester Consulting, which showed 74% of organizations pointing towards **cyberattack to vulnerabilities** implemented during the pandemic that is still impacting their business. This is due, in part, to the difficulties of managing numerous technologies which have increased the exposure of organizations to cyberattacks. One obstacle that remains is a workforce using personal devices. According to the survey, roughly 71% of security leaders do not have visibility into the home networks of employees. Attackers have used this vulnerability to their advantage by targeting remote employees.

New Warnings of Hybrid Working Security Risks

The Financial Conduct Authority (FCA), the UK's largest regulator, **released updated guidance** for organizations that continue to embrace a hybrid working model. The FCA is looking to ensure organizations stay protected by verifying "the lack of a centralized location or remote working" does not increase the risk of financial crime. Organizations will further have to prove there is "satisfactory planning" in identifying new risks while proving they can provide policies and procedures that address and reduce any possibility of financial crime from their hybrid working model. These extra steps from the FCA are welcome news to the financial arena, as they further ensure their hybrid models don't expose them to additional opportunities for attackers to infiltrate their systems.

Voice Cloning Used in Fraud Attack

A court document from 2020 shows how **hackers cloned the voice of a bank customer** to call a bank manager to authorize the transfer of $35 million from the bank located in the United Arab Emirates (U.A.E.). The bank manager followed procedures, and everything seemed legitimate and began the transfer. What the bank did not know was the customer was part of an **elaborate scheme** where the hackers used 'deep voice" technology to clone the customer's speech. In the court documents, the U.A.E. sought the help of American investigators to help track $400,000 that went into US-based accounts. The U.A.E. believes it was an elaborate scheme that involved at least 17 individuals and sent the stolen money to bank accounts all over the world. This case shows how devastating such high-tech deception can be, and the use of AI to create deep fake voices in cybercrime.

Conti Ransomware Attacks Surging

On 23 September, a **report published** by a joint cybersecurity advisory from the US Cybersecurity and Infrastructure Security Agency, FBI, and National Security Agency warned that Conti has so far successfully hit more than 400 organizations based in the US and abroad. The advisory states the Conti Ransomware attacks allow the attacker to steal files, encrypt servers and workstations, and then issues demands for ransom payments. The report offers recommendations to better secure against Conti, such as implementing multi-factor authentication, network segmentation and keeping software up to date.