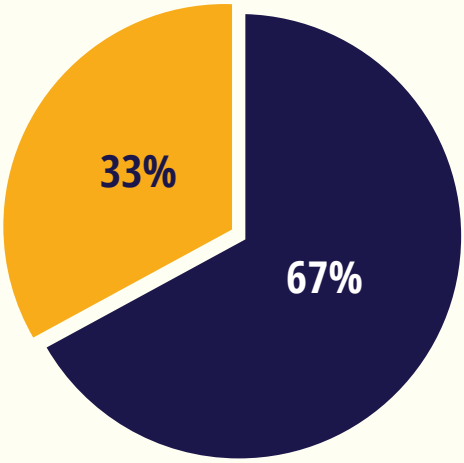
Remote Worker Security Assessment

While 75% of organizations have moved to a hybrid work model , only 21% are confident that their infrastructure security can support long-term remote work with adequate security measures.

In the haste to support the remote workforce at the start of the pandemic, many organizations took the "get it working first" mentality and subsequently sacrificed security. As the remote work model has prolonged, organizations have begun to address security concerns, but sufficient execution is still lacking and security resources are often spread too thin to adequately address gaps.

With increased threats posed by phishing and ransomware in remote work settings, basic endpoint security and traditional cybersecurity training are no longer enough. The attack surface has expanded to every remote device and every email account, and organizations need to identify vulnerabilities and stop abnormal behavior in its tracks. It starts with a thorough understanding of the organization's security posture as it relates to their remote workers and their networks.

Percentage Transmitting Confidential Information



Frequency that users transmit confidential or company information using unauthorized apps (such as IM, Gmail, dropbox, etc.)

The top 4 cyber attacks are aimed at individuals

1. Credential Theft
2. Phishing/social engineering
3. Account takeover
4. General Malware

ClearTone Consulting offers a comprehensive *Remote Worker Security Assessment* to evaluate an organization's risk exposure related to remote workers. With the assessment's results, leaders can create and execute better, prioritized strategies to harden their defenses, educate their staff, and protect their organizational and member data.

This assessment reviews the following areas within the organization against industry best practices:

- Policies
- Procedures
- Technologies and toolsets
- Configurations

The executive report will highlight gaps, offer best practices, and recommend priorities.