Zero-Trust Case

As a potential vector of attack and at risk of phishing, our company should be doing more to monitor and authenticate remote employee devices. By adopting a zero-trust model, we can limit the impact of future breaches by reducing the attacker’s lateral movement. All users are not trusted by default, and any access to company systems must be monitored and authenticated beforehand. Examples of common policies are multifactor authentication and checking device identity. Once they have access, users are limited to roles that restrict access to only essential information, employing the least privilege principle.

The zero-trust model assumes breach, so let’s review what would happen if that same attack occurred. The attacker would first need to have a company recognized device and multifactor authentication credentials to access the company network. If they manage to gain access, their options to execute a lateral attack are limited due to the role the user has. All requests for data access are controlled and encrypted in transit. Their access to other systems in our company is both limited and monitored, providing network administrators to prevent any further attacks on other systems. This will lessen the impact of future attacks while letting employees stay remote.

<https://cyber.gc.ca/en/guidance/zero-trust-security-model-itsap10008>

https://en.wikipedia.org/wiki/Zero\_trust\_security\_model