Information, Privacy and Data Security Post

Addressing the Cyber Risks of Remote Work – Connection Risks

Date: June 11, 2020

This is the third in a three-part series of concise posts geared to risk managers, legal counsel and executives in which we review the major risks associated with remote work and highlight typical controls.

Thus far we have examined the physical security risks of remote work and the risks associated with home computers, personal devices and personal IT services. Here, we deal with the risk that arises when employees access IT services through external networks – often home or public networks that are prone to eavesdropping attacks and that suffer other risks.

The primary means of addressing this risk is to provide for a remote access method that uses cryptography to protect the data flowing between the devices that employees use to receive IT services and the organization's core network. A "virtual private network" is one such a method.

To start, organizations should minimize remote access to IT services and grant remote access only as needed, carefully considering the chosen means of authentication. Granting remote access to some services should not necessarily mean that remote access is granted to all services.

The remote access method must itself be secure. Servers that host remote access applications should be regularly patched, should typically not run other applications and should be carefully monitored for unusual activity. Administrative privileges for remote access servers should be limited, with remote administrator access tightly controlled.

Remote access can be enabled through various technologies that can be deployed in different ways. The strength of security can vary, and there is more than one reasonable option. Organizations should be aware, however, that that the Canadian Centre for Cyber Security and the United States Federal Bureau of Investigation have warned against using Remote Desktop Protocol to enable remote access.

Providing for a secure pipeline through which data can flow is a primary means of enabling remote work. It also can be a cause of security problems that organizations should carefully consider as they increasingly rely on remote work.

Hicks Morley has a leading data security and incident response practice, having helped public sector and other organizations maintain strong data security for over 20 years.