Information, Privacy and Data Security Post

Addressing the Cyber Risks of Remote Work – Physical Security Risks

Date: June 4, 2020

Based on all reports, the global pandemic and the resulting move to “work from home” has caused the cyber risk to organizations to elevate. As organizations move beyond the immediacy of the crises and begin to plan for the medium term, it is a good time to revisit cyber security and, in particular, the risks associated with increased reliance on remote work.

This three-part series of concise posts is geared to organizational risk managers, legal counsel and executives. We’ll review the major risks associated with remote work – physical risks, insecure device risks and connection risks – and highlight typical controls.

The first set of remote work risks are **physical security risks** that arise due to work at home or in other environments that are less physically secure than a workplace. When work is done outside of the workplace, devices can be lost or stolen and sensitive information overseen – means for hackers to gain access to other parts of an organization’s network.

Here are the primary controls for this set of risks:

- Organizations should limit the amount of data stored “locally” on devices, and what is stored locally should be encrypted. Even tighter controls on the use of storage media (e.g. USB keys) are warranted.
- Organizations should consider the use of centralized security management software to enforce security policy on remote devices and to wipe data on devices that are lost or stolen. Organizations should give employees direction on reporting lost and stolen devices and documents.
- Organizations should direct employees to be discreet while working in public and around others. They should also give employees direction pertaining to printing and shredding.

In general, to properly address the physical security risks of remote work, the devices employees use when working outside of the workplace should be as secure or more secure than devices employees use from inside the workplace. This is why the use of home computers and personal devices – “Bring Your Own Device” or “BYOD” – raises special challenges. We look forward to addressing these and related challenges in our next post.

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.