Information, Privacy and Data Security Post

Addressing the Cyber Risks of Remote Work – Personal Devices and Leakage

Date: June 8, 2020

This is the second 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.

In our first post, we examined the physical security risks associated with remote work. Here, we deal with the risk of attaching home computers and personal devices to an organization's network. Such devices can be infected with malware, which represents a direct threat to the computer or device user's information and can lead to additional problems resulting from credential theft or the spread of malware. The use of personal services – e.g., a personal e-mail account and cloud storage account – is a related concern; when work-related data "leaks" onto these services an organization has no security assurances and no control.

The means of dealing with the risk of infection are similar to the means of dealing with the risks of physical insecurity:

- limit the data stored on home computers and personal devices or prohibit local storage altogether
- enforce security policy via centralized security management software so home computers and personal devices are adequately protected, and
- limit the IT services that can be accessed remotely.

The National Institute of Standards and Technology views the risk of remote work from insecure computers and devices as so high that it recommends organizations strongly consider establishing an entirely separate network for delivering services to home computers and personal devices.

Organizations should also establish a rule for use of personal IT services. Organizational work should be done on the organizational network, with personal use of IT services only allowed in limited and precisely defined circumstances.

In our next and last post on addressing the cyber risks of remote work, we address the problem of connecting to a secure network from the outside environment.

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.