Proskauer

Protecting Business Information Assets in the "Work From Home" Environment

New Media and Technology Law Blog on **May 12, 2020**

This past March, many organizations were forced to suddenly pivot to a "work from home" environment ("WFH") as COVID-19 spread across our country. However, many companies did not have the necessary technical infrastructure in place to support their full workforce on a WFH basis. Often, remote access systems were configured assuming only a portion of a company's employees – not 100% of a company's employees – would be remotely accessing the corporate networks simultaneously. In addition, many employees have limited home Wi-Fi capacity that is insufficient to sustain extended, robust connections with the office systems. Networks can then become overloaded, connections dropped, and employees can experience extended latency issues, frozen transmissions and the like.

As a result, many employees are using a work-around — often with their employer's knowledge and approval. They connect their personal devices to their employer's network to download what they need from the network, but disconnect to perform the bulk of their work offline. On a periodic basis and upon the completion of the task at hand, those employees then typically upload or distribute the work product to the organization's network.

Company Business Information Residing on Personal Devices

While this offline work-around may be necessary under the circumstances, it presents certain risks to companies. However, companies can take steps to ensure that important business information created, acquired or discovered "at home" is collected by the company and secured and treated appropriately. Given all of the issues that will likely confound everyone for the remainder of 2020, this is a timely moment to take stock of personal device use, as locally-stored data is likely to be forgotten about as employees begin to return to the office in the near future.

We suggest surveying employees as to their WFH information asset management practices, and, based on their responses, providing appropriate instructions for them to follow.

Preliminary questions to ask all WFH employees include the following:

- Are all work-related materials that are processed on personal devices uploaded and secured properly on the company's file management system?
- Are all copies of such materials (including backup files and any work files residing in the "Downloads" folder) erased from personal devices?
- Are any work-related materials stored on cloud storage sites?
- Are any text and email communications that relate to company business conducted through personal accounts? If so have they since been forwarded in an appropriate way to the company's repository for such communications?
- Are copies of such communications (including email messages/attachments in the Sent and Trash folders) deleted from home devices or web-based communication accounts?
- As a related matter, are hard-copy printouts of business information treated appropriately, including using secure disposal methodologies?

Why are these questions important? Clearly, they are important to ensure that an organization has control over all business information created during the WFH period. But there are other reasons as well:

- Storage of certain information on unprotected personal devices could be, in certain cases, viewed to be a violation of applicable data security laws, and in any case, makes such information vulnerable if the personal devices are lost or stolen.
- Retention of third-party confidential information on a personal device may leave one vulnerable to claims of misappropriation, and in any case, may impair an organization's ability to respond to a business partner's contractual request for the return or erasure of such information.
- To the extent an organization has a document retention policy and supporting system, leaving materials outside of the company's normal information systems means they might not be processed in accordance with company policy. This is important for, among other reasons, managing "litigation holds" and making sure that all appropriate materials are included in a company's back-up, business continuity and disaster recovery systems.

- Retention of company materials on a personal device might allow the individual to retain those materials after such individual is no longer affiliated with the company.
- In some cases, businesses are subject to regulatory requirements to archive and maintain all communications with third parties. These communications would include those sent over personal communication cycles.

Third-Party Access to Personal Devices

Another key question to ask employees is whether the device they use is, or sometime in the future will be, available to others (for example, as a "hand me down")? There are many reasons why this is a particularly important question:

- To the extent the material at issue is third-party information shared with the employer on a "need to know" basis pursuant to an NDA or confidentiality provision in an agreement, the fact that the information is, or may become, accessible to others, may be a breach of that agreement.
- To the extent personally sensitive information is involved, allowing others to access the device may actually constitute unauthorized access under applicable data security laws and trigger breach notification obligations under those laws.
- Disclosure to other users of the device may prejudice the employer's position in subsequent litigation that the information at issue is a "trade secret" and may jeopardize the availability of patent protection under applicable law.
- To the extent a document would normally be subject to attorney-client or other privilege, the fact that the document was accessible to third parties might result in the loss of privilege.

Policy Review

Companies should review applicable policies – including "bring your own device," "work from home," "computer use" and "intellectual property" policies – given the lessons learned during this process. Some of the current WFH practices are likely in violation of some organization's existing policies. Employees should have clear guidance as to how to manage in these unusual circumstances and in the future should such a situation arise again. These policies should build in the safeguards and risk mitigation steps along the way to protect the organization's business information and to ensure that steps are taken to protect third party information in the organization's custody or control.

* * *

These are unprecedented times, and we are learning and adjusting as we go. Some WFH housekeeping will go a long way to ensure that a company can maintain flexibility in these challenging times yet still meet business information management objectives and mitigate risk for the future.

View Original

Related Professionals

- **Jeffrey D. Neuburger**