Practical Technology Considerations for Employers Implementing Work at Home

Article
March 23, 2020

PROFESSIONALS

Katherine M. Hampel
Associate

RELATED SERVICES

Corporate & Securities

As businesses have moved to largely remote operations in response to COVID-19, employers are at an increased risk for exposure of sensitive information and are more susceptible to cyber threats than in traditional office settings. While the potential health effects of the virus were known ahead of businesses opting to enforce work from home protocols, businesses were often forced to employ these measures quicker than desired, with many not being able to update security capabilities to their desired extent. Employees who have never worked remotely are doing so for the first time, some receiving laptops and cell phones from their employers in response to their offices being shut down.

Working from home creates privacy concerns for employers that do not arise in an office full of cubicles and private offices with doors that can be shut to separate employees' spaces from others in the office. When individuals work from home they are sharing their living space with roommates, spouses, and children, and the information that is typically only viewable to them becomes accessible to other people who occupy that shared space. Perhaps most concerning is that users working from home are often working on shared computers, many with roommates and family members sharing logins.

At the same time, hackers are using the concern over the virus and targeted messaging by creating suspicious links related to the virus. They are generating emails that look like they're coming from official sources and offer important information related to the virus that people are anxious to learn about, when in reality these messages contain links that will compromise sensitive information from the devices they are accessed on.

Advice to Employers

Employees using a shared home computer need to work from home must have their own login, and that login should ***not*** have administrative access to the local machine. Make sure all home networks have a firewall and virus protection enabled and up to date.

Remind employees not to open emails from senders and addresses they don't recognize, and to pay extra attention during this time when hackers are trying to take advantage of the situation by creating fake domain names and using

attention-grabbing subject lines that appear to be related to the virus. And if you receive a suspicious looking email, flag and report it immediately. It is important for employers to stay in contact with your employees through multiple channels throughout workdays. Don't just rely on online and email communications, but continue to call and video chat with employees to check-in whenever possible.

Advise employees who are working from home to work on private wireless networks within their homes and not on public networks. Within their private networks, encourage employees to update their security credentials to include stronger passwords and multi-factor authentication where possible. If possible, make sure employees are using company devices when connecting to the employer network, and that they discuss with the company IT department before attempting to connect any private devices to the company network.

Also, pay special attention to the kinds of data your employees are accessing from home. Laws like HIPAA and HITECH, FERPA, and others can impose strict security protocols that may be cumbersome from a home computer and users may seek to circumvent. Emails requiring encryption may be more difficult to access from home and a frustrated employee might look to transmit the data in alternative ways. The potential for data breaches grows the more places the data resides.

Finally, it may be wise to create or otherwise update your computer use policies to make sure they are consistent with the demands of remote operations.