HINSHAW

Implementing a Policy Review to Ensure You Are Protected Under The Computer Fraud and Abuse Act, Part 2: How to Conduct Your Policy Review

3 min read

Oct 13, 2017

By: Ambrose V. McCall

In Part 1 of this series, we discussed the Computer Fraud and Abuse Act ("CFAA") and situations that are readily prohibited by the CFAA, such as when current or former employees gain access to an employer's databases or files to harm the employer or damage its business contacts. We also discussed how a policy review could be beneficial for your workplace. In Part 2, we will discuss how to conduct your policy review and questions you should consider throughout the review in more detail here.

1. Start your policy review with a basic assessment of what type of contractual relationship exists between the employer and current employee.

   Does the employer have a specific written contractual relationship with its employee? Many employers disfavor a specific contractual relationship because they seek the maximum discretion that may be granted to them under an at-will employment relationship.

   But few employers consider that establishing a formal contract with the employee allows the employer to embed provisions that specifically limit the authorized access of contracted employees to employer computers, networks, and digital assets. In employment contracts, employers may also include provisions which limit the employer's exposure to damages for life-time employment claims or retaliatory discharge claims.

   For employers with at-will employees, review your personnel policies in a big picture scenario. Does the policy that you plan to use to establish an exceeding authorized access claim appear in a set of policies that state in an all-caps and bold font proclamation that all the policies are non-contractual and non-binding?

If so, does the policy that limits employee authorized access to an employer's computer, networks, and digital assets appear in a separate memo, signed by the employer and employee, and explicitly say that the terms of the limiting access policy adds to, amends, or modifies the existing at-will employment relationship?

2. Determining whether there are any processes in place to remind incoming and existing employees that they lack access to certain employer computers, networks, and digital files.
   - Do managers or supervisors have and document meetings within their departments to remind employees that they lack access beyond a certain data set of employer digital assets?
   - Is it simply assumed that no employees download what they can obtain access to onto thumb drives or other media, or email documents to themselves at non-work email addresses?
   - Has anyone informed the administrative staff to senior management in a data sensitive area that they are absolutely not to grant access to personnel outside of their line of managerial authority?
   - In the event of litigation, if there are no post-hiring memos, meetings, or demonstrations, the employer may be vulnerable to a procession of witnesses and documents that may show how business tasks were actually conducted by the employees. The evidence may overwhelm a single signed policy that is part of a non-binding HR handbook. Moreover, an employer seeking a temporary injunction may lack a coherent explanation when asked by a judge what steps it took to explain, gain consent, implement, and monitor employee compliance with a policy it contends limited digital access of a current (and now former) employee.
3. Determine what information and documents the employee has access to.

   What the employer hears from its IT department about password levels and encryption security remains very significant. But upon donning the employee computer, password, tools, and security badge in question, and taking a digital tour, what does the employer find that a typical employee in the reviewed area can access in the employer's digital world?

   Without obtaining such granular knowledge, and finding out what side agreements in the workplace may have been made between employer departments and employee staff, the employer's management may not have a full picture of what access was already granted to various employees. An employer that conducts a holistic review may find that its current employees already have full access to everything in the employer's digital vault. But until such measurements are taken, employers will have challenges in showing that certain employees clearly exceeded their authorized access to employer computers as defined in the CFAA.

   For employers who want to enlist the helpful assistance that the CFAA may provide them, the key is to create and install a process with a team of legal, management, HR, and IT personnel. Leaving out any component may prove fatal to both protecting employer digital assets and to seeking relief under the CFAA.

Hinshaw & Culbertson LLP is a U.S.-based law firm with offices nationwide. The firm's national reputation spans the insurance industry, the financial services sector, professional services, and other highly regulated industries. Hinshaw provides holistic legal solutions—from litigation and dispute resolution,

and business advisory and transactional services, to regulatory compliance—for clients of all sizes. Visit www.hinshawlaw.com for more information and follow @Hinshaw on LinkedIn and X.

Topics

CFAA