Security Breached – Tips for Mitigating and Protecting Private Information from Inside and Outside Threats

Insights
3.26.18

If you're going to demote or terminate your in-house tech expert, you should plan that event very carefully.

Our firm is now helping a client with damage control and data recovery upon discovering – a week after their former Chief Technology Officer (CTO) had resigned but ***six months after*** he'd been demoted to a lesser role -- that the CTO had created a back door for himself to the client's servers and had spent those last six months of his employment accessing, downloading and storing emails of the client's top executives, and its most important vendors. These stolen emails contain personal financial information, such as bank account numbers, personal health information, bank routing information for personal accounts of the client's top executives, including the CEO and two board members. The former CTO also had accessed and downloaded other proprietary corporate information, including bank routing numbers for several of the client's most important vendors, and other private information. At a minimum, the executives and their vendors will need to change their banking and other private, personal information, at some if not significant expense, and no less heartache.

While you might think the Chief Technology Officer would have had such access authorized, he did not. He most certainly exceeded his authorized access, and did so without requesting or obtaining permission either from the client, the executives, or the vendors. Additionally, as part of his resignation, the client and the former CTO arranged a "consulting agreement," under the terms of which he was permitted to keep and use his company-issued laptop.

After the new CTO discovered the unauthorized back door access channel, we scrambled to draft and file a request for an emergency, *ex-parte* Temporary Restraining Order against the former CTO from the nearest U.S. District Court, for violations of the Computer Fraud and Abuse Act and the Defense of Trade Secrets Act, and to secure the return of the company laptop.

The Court granted the emergency TRO, which is good for 14 days, and the client has retrieved the laptop. However, the process server hired to deliver the court papers to the former employee and to retrieve the laptop was required to wait for 45 minutes while the former employee "searched" for it in his own home. While the process server waited, with the former employee out of his eyesight, it is entirely possible this former CTO deleted or attempted to delete compromising information still on

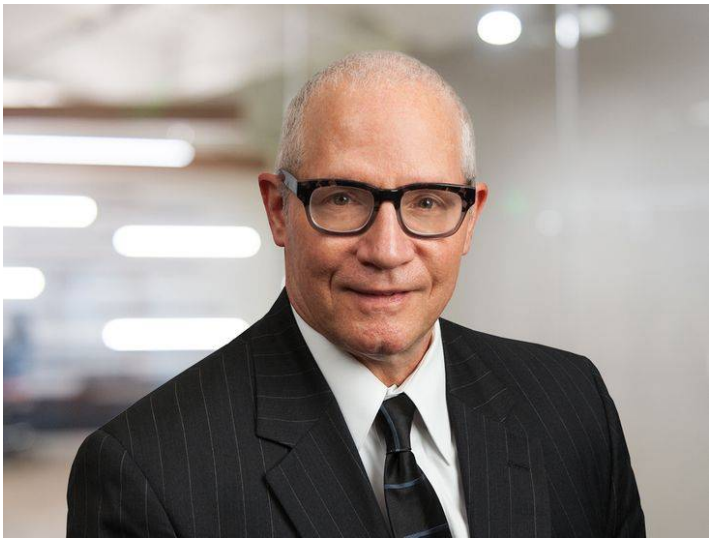
Copyright © 2025 Fisher Phillips LLP. All Rights Reserved.

the laptop's hard drive. The computer is now in the hands of a forensic computer expert who can examine it thoroughly.

The point of this discussion is simple – we as employers ought to know by now that our technology-savvy employees, especially our in-house technology experts, are quite able to figure out ways to steal, use or corrupt our electronic information. Rather than wait until ***after*** they've departed to determine if they've done anything that can harm us or our other employees, we should plan to conduct such an inquiry ***before*** we demote, re-assign, otherwise discipline or terminate any employee. This is especially true for those with the technical expertise to engage in electronic misconduct. That way, if we find misconduct has occurred, we still have some control over the employee and can diminish or negate the harm before the employee is gone from our premises. It is a more timely and cost effective method of protecting our, and our employees', privacy and private information.

Access the employee's desktop or laptop (or any other company-issued device such as a tablet or smart phone) outside their presence, utilizing an independent forensic expert to "image" the device's hard drive, then examine it. Be sure to maintain and record a clear chain of custody of the device. If there is data on the device the employee should not have, you of course can question them about it. If it looks like they've moved, copied, or compromised data, your forensic expert should be able to tell you. If they've corrupted data, you might be able to mitigate the damage while you still have them in front of you, to be questioned. After they're gone, your only access to them may be a subpoena, or a lawsuit.

Related People



Andrew Froman
Partner
813.769.7505
Email

Copyright © 2025 Fisher Phillips LLP. All Rights Reserved.