Buchalter Client Alert Covid-19: Cybercrimes

The COVID-19 pandemic have opened the floodgates of cybercrime, as hackers are exploiting distracted workers adjusting to working from home. This alert highlights a number of these issues and its relationship with California legislation:

RISE OF COVID-19 THEMED PHISHING EMAILS

As the COVID-19 pandemic continues to spread throughout the United States, an increasing number of states are issuing orders that restrict a person's ability to leave their home for non-essential tasks. These restrictions have shuttered offices across the country. In response, many businesses have instituted "work-from-home" policies for the foreseeable future, giving employees remote access to the computer systems so they can remain at home to comply with shelter-in-place orders. As a result, many IT departments have been stretched thin handling the logistics of moving nearly all business operations to allow for remote access.

This transition period has exposed companies to various forms of cyber-attacks which have been on the rise. Hackers have posed as the Center for Disease Control and Prevention and the World Health Organization attempting to get people to click on dangerous links for more information on the virus. In fact, recently the U.S. Health and Human Services Department suffered its own cyber-attack on its computer system.

Specifically, companies should be on the watch for several types of emails which have become more prevalent amidst the global pandemic:

1. Business email compromise attacks – where a hacker will create a spoof email which makes it appear that it is coming from a senior colleague (often a CEO or CFO). The email attempts to trick the victim into making a money transfer or "payment" to a difficult-to-trace bank account associated with the hacker.
2. Ransomware attacks – in which a hacker will gain access to the victim's computer system and lock the victim out and demand digital currency in exchange for regaining access. These are often carried out by including a malicious attachment or embedded link to a phishing email.

There is a high volume of online communication as a result of employee transition to remote access. Additionally, many businesses have been reaching out to their employees and customers to give updates on their business as a result of the current environment. This potentially gives hackers additional opportunities to try and carry out their malicious attacks. Companies should be warning

their employees of the threat of these attacks, as well as reminding them of their policies and procedures when receiving emails asking for money, clicking links, or downloading attachments.

IN THE EVENT OF A BREACH

As a reminder, in California there are two statutes that identify what a company should do in the event of a data breach: Civil Code section 1798.29 (for state agencies) and Civil Code section 1798.82 (for private businesses). In both, the business needs to disclose the breach of the security system "in the most expedient time possible and without unreasonable delay…."

Once a company discovers that its data might be compromised, it must begin its investigation as soon as possible in order to determine the affected parties and provide full notice as laid out in the statute. If the breach affects more than 500 California residents, a copy of the breach notification must also be sent to the California Attorney General.

THE ROLE OF THE CALIFORNIA CONSUMER PRIVACY ACT IN BREACH INCIDENTS

The California Consumer Privacy Act ("CCPA") is a comprehensive data privacy statute signed into law June 2018 that became effective January 1, 2020. It provides for a limited private right of action to California consumers when their "nonencrypted and nonredacted personal information" is "subject to an unauthorized access, exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures." Effectively, this means that a victim of a security breach can potentially sue the company whose data has been accessed by a bad actor if the company did not implement and maintain reasonable security procedures. The statute also provides statutory damages of "not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater." In the event of a class-action lawsuit, the statutory damage award could be very costly.

While the legislature has not clarified what "reasonable security procedures" are, there are steps companies can take to better equip themselves from the threat of a cyber-attack. These include, but are not limited to:

- Periodic risk assessments;
- Internal/external penetration tests; and
- Regular cyber-security trainings for your employees.

Buchalter understands that the pandemic has caused companies to act with extra caution with respect to the health and well-being of their employees and customers. However, it is also important to remain diligent with respect to the company's computer systems and personal information to avoid becoming the victim of a cyber-attack.

If we can be of assistance and to discuss various options and specific situations, please feel free to contact our Attorneys listed below.

Matthew Seror
Shareholder
(213) 891-5731 or mseror@buchalter.com

Weiss Hamid
Attorney
(213) 891-5087 or whamid@buchalter.com