The Work Week

Bassford Remele Employment Practice Group

October 9, 2023

Welcome to another edition of *The Work Week with Bassford Remele.* Each Monday morning, we will publish and send a new article to your inbox to hopefully assist you in jumpstarting your work week.

Bassford Remele Employment Practice Group

Who Bears the Liability When an Employee's Email Account Gets Hacked?

It is probably your company's worst nightmare – one employee can click on a malignant email link and **poof** a hostile entity controls the employee's email account. Such a hostile actor can compromise the employee's entire digital identity and potentially any person's digital profile who interacts with the compromised account. If this employee works in accounting or with highly sensitive data, the consequences are catastrophic. From the interception of corporate funds to document management systems being hacked, to massive data breaches, employers must be hyper vigilant to avoid disastrous outcomes.

In a new era of A.I., "deep fakes," and cyber warfare, it is essential for employers to revamp their policies, procedures, training, and a response protocol in case a cyber attack occurs. Such attacks are not just speculative—they are a reality.

For example, in *Bohnak v. Marsh & McLennan Companies, Inc*., 79 F.4th 276, 283 (2d Cir. 2023), an employee brought a class action lawsuit when an unauthorized actor used a third party's software which was utilized by Defendant Marsh & McLennan to capture the Plaintiff's personal identifying information, ("PII") including her name and social security number. Plaintiff Bohnak brought a nationwide class action lawsuit against Marsh & McLennan, alleging the company failed to adequately protect the PII of the Plaintiff and Class Members, failed to warn the Plaintiff and Class Members of Defendant's inadequate information security practices, and failed to effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Although Plaintiff did not allege a direct injury from the hacker's use of her PII (because she did not yet have one), the appellate court recently found that Plaintiff still had standing to bring the lawsuit, concluding that the "risk of future injury is sufficiently concrete to constitute an injury in fact for purposes of a claim of damages."

As *Bohnak* illustrates, cyber attacks are a reality and present potential liability for employers. Below are three concrete steps employers should take to mitigate their risk in the ever-changing cyber environment.

1. **Institute Mandatory and Comprehensive Cyber-Security Training for Employees**

An employer should mandate cyber-security training for employees who deal with sensitive data or are interacting with company data on a regular basis. Educating employees on suspicious emails and pop-up windows will help mitigate the likelihood of employees clicking on links that might allow a hostile actor access into that employee's email account. Additionally, employees should be changing their passwords regularly and locking their computers whenever they leave their offices. Cyber-security training can inform employees on what to look out for to prevent employees from being digitally compromised.

2. **Develop Procedures and Policies to Prevent a Cyber Attack**

Employers should have cyber-security policies that insure two-factor authentication for employees logging into company databases. In addition, employers should mandate cyber-security training for employees, implement data-management practices, require employees to not use public Wi-Fi (*i.e.,* a network-security policy), and maintain a vendor-management policy—and these polices are just a starting point. To ensure your company is actively preventing a cyber attack and to avoid liability, employers need to develop comprehensive procedures and policies to prevent cyber-attacks.

3. **Maintain a Response Protocol in the Event of a Cyber Attack**

Finally, in the event of a cyber attack, employers must maintain a response protocol for notifying those affected by the breach and for stemming the attack as soon as possible. For example, a policy outlining a step-by-step response for who to contact, detect and isolate affected systems and hardware, and to preserve data and information, is essential for having an effective response to a cyber attack. Instituting a response policy will streamline the response for all parties involved.

Bassford Remele is your trusted partner for navigating new developments in employment law, including the intricate realm of cyber-security liability. In addition to our Employment Law practice group, Bassford also has a robust Data Privacy and Cyber Security practice group. If you're seeking guidance, have questions or concerns in the realm of cyber-security liability, our team of experienced attorneys at Bassford Remele is here to assist you.

LEARN MORE ABOUT OUR EMPLOYMENT PRACTICE »»
