akerman

Prepare NOW to Manage Your Workforce Through a Cyberattack

June 27, 2022

It is every employer's worst nightmare: an unsuspecting employee receives an email in the early morning from an individual claiming to be his supervisor. The email asks him to follow up on an urgent work assignment that needs his immediate attention. With multiple deadlines fast approaching, he does not think twice. He opens the email and attached file, and prepares to work. Within minutes, the entire system — including all confidential and proprietary data, timekeeping records, and payroll records stored in it — becomes inoperable and shuts down. The attacker delivers a single message to the employer: pay the ransom in exchange for the data or risk losing all the files.

Ransomware attacks are on the rise, and employers are increasingly being targeted. By some estimates, in the first seven months of last year alone, reports of ransomware attacks showed a staggering 62 percent year-over-year increase. Ransomware is a form of malicious software that can infect and lock down a target's network. While some malicious actors demand ransom in exchange for decryption software, others simply steal the company data regardless of whether a ransom is paid, often leaving victims with no way to tell what the attacker has accessed or taken. Needless to say, ransomware attacks can disrupt operations across the company and result in the loss of trade secrets, sensitive commercial information, personal data, and even medical documents.

More than ever before, it is imperative for employers to stay alert, understand the relevant laws, and

Related Work

Labor and Employment
Wage and Hour

Related Offices

Los Angeles

HR Defense

Akerman Perspectives on the Latest Developments in Labor and Employment Law

Visit this Akerman blog

implement both preventative measures and contingency plans.

Federal and State Laws Counsel Vigilance

Ransomware attacks can instantly cripple a company's ability to manage its operations—payroll, timekeeping, and document retention—and the consequences can prove costly. In most states, payroll and timekeeping procedures are governed by both federal and state law. The Fair Labor Standards Act (FLSA) is the primary federal law governing wage and hour standards for most workers in public and private employment. The FLSA does not require wages to be paid weekly or on a particular day of the month. However, once the employer designates specific payroll dates, it is required adhere to its schedule. Failure to do so can expose the company to claims for unpaid wages and, in some cases, liquidated damages.

Many states impose more stringent requirements. For example, in New York, manual workers must generally be paid on a weekly basis, while clerical workers must be paid at least semi-monthly. In California, employers are required to pay most non-exempt employees on at least a semi-monthly basis on designated paydays each month.

Employers are also required to implement compliant timekeeping practices. While neither state nor federal law generally require employers to use a particular method of timekeeping, companies must ensure that their system accurately, and reliably, records all hours worked, and that the underlying time records are preserved.

All employers are required to maintain payroll records for a minimum of three years under federal law. But some states may require companies to maintain records for a longer period. In fact, in most states, the best practice for employers is to retain payroll records for at least four years (up to six years

in New York), and benefits-related documents for up to six years.

Importantly, the penalties for not maintaining accurate time and payroll records fall on the *employer*, not the employee. In litigation, an employee can prove unpaid wages through witness testimony, including their own self-serving testimony. The burden is then on the employer to establish the precise number of hours worked or to negate the employee's evidence. If an employer fails to produce the worker's payroll or timekeeping records, the case may very well be decided on the employee's own evidence.

Develop a Crisis Management Plan

In today's digitized world, workforce management software and cloud-based services are becoming the new normal across public and private markets. Consequently, employers are well advised to implement both a contingency plan, and preventative measures, to respond to cyberattacks. Consider the following:

1. **Develop and test an incident response plan.** Time is of the essence in the minutes after a cyberattack. Make sure that your organization has developed a plan to respond to cybersecurity incidents and test the plan regularly. Among other things, the incident response plan should identify the employees who will be part of the incident response team and assign at least one person the responsibility to help the leadership navigate through the incident and, to the extent possible, mitigate any data losses as quickly as possible. Your plan should also define the payroll and timekeeping procedures that will be followed in the moments after a cyberattack. Most employers will need to have their employees temporarily switch to manual timekeeping or some other offline system. Discuss that system with your team, review it with all new workers as part of

their onboarding process, and periodically go over it with your staff.

2. **Train and test your workforce on phishing.** Phishing refers to the fraudulent practice of sending emails to trick the recipient into revealing sensitive information or to deploy malicious software on a network. Many companies implement "simulated phishing" in the form of internal emails or urgent requests to provide targeted security awareness training. This can be a useful way of educating and training new and current employees on the latest cyber threats.
3. **Review your Services Agreement**. Many employers engage third party companies to process, manage, and store all of their timekeeping and payroll records. If that is the case for your company, review the services agreement with your payroll provider and clarify the scope of your company's, and the provider's, responsibility with respect to recording and storing personnel information. If you are not satisfied with those provisions, propose changes and negotiate an agreement that works for your organization.
4. **Build redundancy into your payroll system.** Understanding that cloud-based systems (or any electronic systems for that matter) are not perfect, employers should implement at least one or more backup recordkeeping systems. Consider backing up all personnel records in an alternate, encrypted, and offline system.
5. **Review and revise employee manuals/handbooks to address emergencies**. To the extent you have not done so already, revise your employee manuals/handbooks to describe how your organization will manage payroll and timekeeping, as well as any other personnel issues, in response to a cyberattack. If you are in a state that does not require payroll to be paid at statutorily defined intervals, add a disclaimer in your manuals/handbooks explaining that the payroll dates are subject to change in the event of

an emergency, and that in such cases, payroll will be made on the next practically available day.

Ultimately, the effectiveness of a company's response will largely depend on its preparedness and dexterity in switching between different workforce management systems, as well as its understanding of its own limitations. In light of the increasing rate of cyberattacks, you should ensure that those plans have been thoroughly vetted and discussed with all decision makers, HR, and IT personnel.

For questions regarding employer responses to cyberattacks, and all other wage and hour issues, contact your Akerman attorney.
