NEXSEN | PRUET

Kronos Catastrophe: What Employers Can Do to Avoid Panicked Payroll Practices

Related Professionals

Bridget A. Blinn-Spears
919.678.7593
BBlinn-Spears@nexsenpruet.com

Christy L. Rogers
803.540.2173
CRogers@nexsenpruet.com

Practices

Employment & Labor Law

Article
01.10.2022

Ransomware locked up time records for thousands of companies across the country last month, and those records remain unavailable. Ultimate Kronos Group ("Kronos") is a well-known workforce management platform used to track employee scheduling, attendance, and payroll. On December 11, 2021, Kronos announced that one of its cloud-based time and attendance systems had been exploited by hackers. Kronos has been working to repair the damage and regain system functionality, but in the interim, a complete shutdown has occurred, blocking access to electronic records of employers across the country. While the days lagged on, frustration turned to panic, as Kronos admitted the ransomware attack could render the system inoperable for several weeks as employers scrambled to track employee hours, process payroll, distribute year-end bonuses, and accurately track vacation usage for the holidays.

While employers implemented stop-gap measures, many expressed disbelief that a company of Kronos' size did not appear to have a contingency plan for its customers, many of whom exclusively relied on the platform for payroll and attendance-related functions. However, ransomware attacks are not a novel threat, and other major businesses were also targeted in 2021, resulting in disruption to critical supply chains. Colonial Pipeline was the victim of a ransomware attack in May that affected the flow of oil all across the country. Just one month later, JBS USA, a large meat-processing vendor, was hit by a ransomware attack that severely hindered the company's ability to package and process meat products. All told, reports of ransomware attacks to the FBI's Internet Crime Complaint Center during the first half of 2021 represented a staggering 62% year-over-year increase.

Like Colonial and JSB, the impact of Kronos' ransomware attack was widespread, resulting in the sobering realization that without the use of its electronic recording keeping system, many employers were completely unprepared to handle the logistics of timekeeping and payroll requirements for their workforce. More significantly, employers were also faced with the reality they might be unable to meet their legal obligations

with respect to recordkeeping and pay.

Kronos confirmed in early January 2022 that the hackers had also disabled its ability to access its backup data. Kronos now is rolling out individual timelines for system and data restoration for each of its customers. In light of the vulnerability of these electronic systems, employers must anticipate unexpected failures and be prepared to implement any needed corrective measures or alternative processes to ensure continued legal compliance and minimize disruption to the business. So, what are the lessons learned from the Kronos attack?

Know the Law

First, make sure you understand what the law actually requires, so you can verify that during times of outage or crisis you are complying with all obligations. For the Kronos outage, the key compliance areas are tracking and maintaining time records and accurately and timely paying wages. The Fair Labor Standards Act ("FLSA") is the federal wage payment law that establishes minimum wage and overtime pay. The FLSA also sets forth certain recordkeeping requirements, which mandate the retention of specific documents related to each non-exempt employee's pay. These records include: (1) time and day of the week when the employee's workweek begins, (2) hours worked each day, (3) total hours worked each workweek, (4) basis on which employee's wages are paid (e.g., per hour, per week, etc.), (5) regular hourly pay, (6) total daily or weekly straight-time earnings, (7) total overtime earnings for the workweek, (8) all additions to or deductions from the employee's wages, (9) total wages paid each pay period, and (10) date of payment and the pay period covered by the payment.

Federal law requires that all payroll records must be preserved for at least three years, and records on which wage computations are made (i.e., time cards, wage rate tables, work and time scheduled, records of additions and deductions from wages) must be retained for at least two years. State laws may require longer record retention periods and also increase minimum wage and overtime obligations. Notably, these recordkeeping obligations apply to *employers*. Employees have no such obligation, and if they claim they were paid improperly by a company that lacks the appropriate records, employees can rely on evidence of their own recollection of hours to prove those claims. Employees often recall their longest and hardest weeks at work, which may (intentionally or unintentionally) inflate their claims for unpaid hours.

While the FLSA does not address the timing of wage payment, most states have wage payment laws that penalize employers for late wage payments. Thus, employers also should familiarize themselves with the applicable state wage payment law in any jurisdiction(s) where their company has employees, as those statutes set forth further requirements and typically include potential fines for failure to timely and accurately pay wages.

Have a Plan

While most companies recognize the need for a business continuity plan for weather emergencies or catastrophic damage to buildings or records, fewer have crisis management plans that address disruption of payroll-related functions. Timely and proper pay is not only critical to employees, it is vital to smooth, efficient, and litigation-free business operations. Accordingly, employers should maintain a written plan that addresses the following:

→ Identify key components of electronic or cloud-based recordkeeping that are potentially vulnerable to attack;

- → Be sure you have contact information for your customer service representative point of contact so you can swiftly address issues and obtain assistance to get your system's functionality restored as quickly as possible;
- → Determine what system or process will be used in the event of a data crash for any components of that system (e. g., accessing electronically stored information locally, handwritten time cards, time tracking spreadsheets, state-specific pay requirements, manual check distribution);
- → Set out a process for creation and retention of scheduling and/or shift assignments, if applicable, and how employees will be notified of their work schedule each workweek;
- → Describe how any changes in procedure will be communicated to employees and managers;
- → Identify a central point of contact for employees who experience errors with their pay; and
- → Consider keeping your own backups of timekeeping and payroll records maintained in third-party systems.

Conclusion

Regardless of whether they were directly affected by the Kronos ransomware attack, employers have the opportunity to plan ahead for catastrophic outages of timekeeping and payroll systems. As companies are increasingly dependent on technology and hackers are ever more creative, a proactive approach can help avoid panic when disaster does strike.