

# Commercial Risk Advisor

December 2018

---

*The number of ransomware attacks has risen 32 percent since August. Even a small attack can cost your business thousands and interrupt your regular operations.*

---

Provided by:  
LaPorte



---

## Ransomware Attacks are More Common Than Ever

---

Although hackers can use a growing list of cyber attacks to endanger businesses, one of the costliest and most common is ransomware. And, according to a new report from Beazley, the number of ransomware attacks has risen by 32 percent since August.

Ransomware relies on social engineering schemes or other common cyber attacks to install malware onto a network. Then, users are “locked out” until they pay a high ransom—usually in an anonymous cryptocurrency. These attacks are especially common because it’s easy for hackers to use automated programs to target multiple networks at once, and the high costs associated with business disruptions pushes many employers to quickly give in and pay the ransom.

Even a small attack can cost your business thousands of dollars. Keep these best practices in mind to secure your network and ensure your business stays up and running:

- **Perform an audit to see how long your business can afford to lose access to its network.** Your unique circumstances will affect how long you have to respond to an attack, and discovering this time frame can help you develop the rest of your response plan.
- **Establish a program for software updates.** With enough time, hackers can break through even the newest software. However, turning on automatic updates or establishing a program to ensure you have the newest software available will give you access to the latest security fixes from developers.
- **Keep physical backups of critical data.** Many businesses take online data storage for granted and are helpless once a ransomware attack locks their critical information away. Make sure to store your most important data physically, such as on a USB or hard drive.

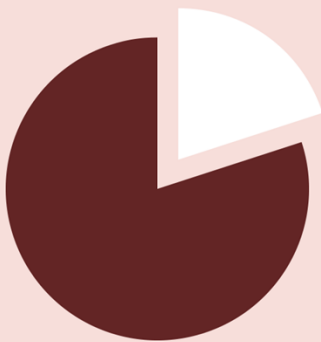
Businesses lose an average of **\$8,500 every hour** they're disrupted by a ransomware attack.



A company is targeted by ransomware **every 40 seconds**.



**20%** of small and medium-sized businesses that pay ransoms never get their data back.



Source: Kaspersky Lab

## NLRB Proposes Changes to the Joint Employer Standard

The National Labor Relations Board (NLRB) has standards for determining when multiple employers are responsible for a single employee. Now, the agency has proposed changes that would establish a stricter standard for determining joint employer status. These changes could have a large impact on NLRB compliance in many industries, as businesses with joint employees can be held liable for labor practices committed by another employer.

Currently, joint employer status is established when a business has “sufficient” control over a worker’s essential terms and conditions of employment, regardless of whether the employer actually exercised its right of control. However, critics argued that sufficient control isn’t a clear definition and that many businesses aren’t aware when they’re in a joint employer scenario.

Under the current standard, the NLRB can determine that even indirect influence or common contractual reservations of authority establish joint employment. Unfortunately, businesses can then be found liable for another employer’s unfair labor practices. The proposed changes would establish a clearer standard for establishing these situations:

- Two employers must share or codetermine an employee’s essential terms and conditions of employment, such as hiring, firing, discipline, supervision and direction.
- An employer must possess and exercise substantial, direct and immediate control over the essential terms and conditions of employment of another business’s employee in a manner that isn’t limited and routine.
- Indirect influence and contractual reservations of authority would no longer establish joint employer status.

The NLRB proposed these changes in order to make the standard more predictable and prevent third parties that don’t have an active role in critical terms of employment from entering into a collective-bargaining relationship with another business’s employees.

For more information on compliance with the NLRB and protecting your employees, contact us at (503) 239-4116 today.