CYBERRISKS&LIABILITIES

Ransomware Considerations for Board Members

Organizations of all sizes and sectors are facing increased cybersecurity risks. Specifically, ransomware attacks—which leverage malware to compromise a victim's data and demand them to make a large payment to recover it—have quickly become a rising threat across industry lines. In fact, recent research found that these types of attacks have surged by 150% in the past year alone, with the average amount paid by victims jumping by over 300%. Such attacks have also become more sophisticated over the years as cybercriminals have developed a wide range of different ransomware-use techniques.

In light of these advancing cyber concerns, it's important for board members to be actively involved in developing and promoting effective workplace cybersecurity measures—especially as it pertains to ransomware attacks. By involving senior leadership in such initiatives, organizations can foster a culture of cybersecurity awareness and bolster their preparedness against cyber threats. Here are five key questions that board members should discuss to help their organizations stay resilient against ransomware attacks.

1. How can our organization better detect ransomware threats?

Before a ransomware attack can occur, a cybercriminal has to gain access to their target's network, systems or data. Once a cybercriminal gains this access, an extended length of time—also known as "dwell time"—typically passes before the ransomware is deployed and the attack actually begins.

With this in mind, organizations that are able to detect potential ransomware threats during dwell time rather than at the onset of an attack can stop such incidents before they even start. The following measures can help board members ensure the earliest possible detection of ransomware concerns within their organizations:

- Keep updated records of all workplace technology to understand where ransomware threats could arise.
- Equip all workplace technology with antivirus and malware detection software. Update this software regularly.
- Have critical technology, systems and data consistently monitored for suspicious activity. Make sure the employees in charge of these monitoring procedures are properly trained to do so.
- Establish thresholds for when employees should notify senior leadership of ransomware threats.
- Provide all employees with clear ransomware reporting protocols.

2. What can our organization do to minimize the damages in the event of a ransomware attack?

When ransomware attacks occur, it's vital for impacted organizations to do everything they can to limit the damages. In particular, board members should prioritize these procedures:

- Keep data encrypted. This practice will make it significantly harder for cybercriminals to compromise data during a ransomware attack.
- Restrict employee access to workplace technology, systems and data. Only allow access on an as-needed basis.
- Require employees to use proper credentials and multifactor authentication when accessing workplace technology, systems and data.
- Consider keeping different workplace networks

Conrey INSURANCE BROKERS & RISK MANAGERS

separated to prevent cybercriminals from gaining full access after attacking a single network.

3. Does our organization have an effective cyber incident response plan in place?

Cyber incident response plans are one of the best tools for helping organizations react appropriately and mitigate losses amid cyberattacks. Board members should work closely with workplace leaders across departments to develop sufficient cyber incident response plans for their organizations. Generally speaking, an effective cyber incident response plan should outline:

- Who is part of the cyber incident response team (e.g., board members, department leaders, IT professionals, legal experts and HR specialists)
- What roles and responsibilities each member of the cyber incident response team must uphold during an attack
- What the organization's key functions are and how these operations will continue throughout an attack
- How any critical workplace decisions will be made during an attack
- When and how stakeholders should be informed of an attack (e.g., employees, customers, shareholders and suppliers)
- What federal, state and local regulations the organization must follow when responding to an attack (e.g., incident reporting protocols)
- When and how the organization should seek assistance from additional parties to help recover from an attack (e.g., law enforcement and insurance professionals)

Take note that cyber incident response plans should be evaluated and updated regularly to ensure effectiveness. Various activities can be implemented to assess cyber incident response plans—including tabletop exercises and penetration testing.

4. Does our organization's cyber incident response plan adequately address ransomware attacks?

Cyber incident response plans should address a wide range of possible attack circumstances. That being said, it's important for board members to ensure that ransomware attack scenarios are properly accounted for within their cyber incident response plans.

Specifically, board members must determine whether or not their organizations will make ransom payments to cybercriminals—particularly when the compromised data is sensitive in nature or critical to operations. Keep in mind that cybersecurity experts typically advise against complying with ransom demands, seeing as there is a chance that cybercriminals could take the ransom money and not recover the compromised data or leverage it in future attacks.

Further, board members must ensure their organizations are prepared for the lengthy recovery process that often accompanies ransomware attacks. In some cases, it can take several weeks or months to recover compromised data. During this time, board members must have plans for keeping their organizations functional and minimizing reputational damages.

5. Are all data backup protocols within our organization sufficient in protecting against ransomware threats?

Backing up important data can help organizations maintain access to key files and information during cyber incidents. However, poor data backup protocols can easily be exploited by cybercriminals, subsequently resulting in ransomware attacks. As a result, board members should ensure their organizations follow these data backup security procedures:

- Conduct data backups on a routine schedule. Consider backing up critical data more frequently.
- Store data backups offline and in a separate location from other workplace systems and networks.
- Only allow trusted and qualified employees to perform data backups.

For more risk management guidance, contact us today.